Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Responding to Personally Identifiable Information (PII) Breach Procedure

1. PURPOSE

This procedure identifies the steps the U.S. Environmental Protection Agency (EPA) employees will take to respond to suspected or confirmed breaches of Personally Identifiable Information (PII). In addition, this procedure sets out the roles and responsibilities for reporting and responding to PII breaches so that Agency officials, employees and other individuals may respond quickly and effectively to each type of breach and its circumstances.

2. SCOPE

This procedure applies to Agency employees, grantees and contractors and supplements other Agency procedures, identified in Section 8, for protecting PII and responding to incidents regarding the security of such information.

3. AUDIENCE

The audience is all EPA employees, contractors, grantees and others performing work on behalf of the EPA.

4. BACKGROUND

On May 22, 2007, the Office of Management and Budget (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. The EPA established the Breach Notification Team (BNT), a core group of Agency senior leaders to respond to breaches of PII. 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 of PII incidents, the Agency established the Breach Evaluation Team (BET), the Breach Evaluation Team Executive Committee (BET EX) and BNT. The BET reviews suspected or confirmed breaches of all PII and Sensitive Personally Identifiable Information (SPII) and decides the Agency’s response to breaches of PII (non-SPII). The BET provides the BET EX recommendations

for Agency responses to breaches of SPII. The BET EX acts on behalf of the BNT to respond to suspected or confirmed SPII breaches. The BNT convenes only in circumstances defined later in this procedure. For the definition of roles and responsibilities, see Section 7. For the definitions of PII, SPII, and other terms used in this procedure, see Section 9.

M-17-12 set forth the policy for Federal agencies to prepare for and respond to breach of personally identifiable information (PII). It includes a framework for assessing and mitigating the risk of harm to the individual potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. In reference to M-17-12, agencies should be consistent in the way they prepare for and respond to breach by requiring common standards and processes. It provides agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and analysis of the risk of harm to potentially affected individuals.

5. AUTHORITY

- OMB Memorandum, M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017.
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, December 23, 2016.
- OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016.
- OMB Memorandum, M-16-14, Providing Comprehensive Identity Protection Services, Identity Monitoring and Data Breach Response, July 1, 2016.
- OMB Memorandum, M-11-02, FY 2010 Sharing Data While Protecting Privacy, November 3, 2008.
- OMB Memorandum, M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.
- OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notifications, September 20, 2006.
- OMB Memorandum, M-06-19, Reporting Incidents Involving PII and Incorporation of Cost for Security in Agency Information Technology Investments, July 12, 2006.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006.
- OMB Memorandum, M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006.
- OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, February 11, 2005.
- OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data Protecting Personal Privacy, December 20, 2000.

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

6. PROCEDURE

The EPA's Chief Information Officer (CIO) is designated as the 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. The Chief Privacy Officer (CPO) has been designated to carry out the SAOP's responsibilities for the National Privacy Program (NPP). The daily operations of the NPP have been delegated to the Agency Privacy Officer (APO).

A. Breach Response Plan

Develop and implement a breach response plan which includes the following elements:[1][2]

- Breach Evaluation Team (BET).
- Breach Evaluation Team Executive Committee (BET EX).
- Breach Notification Team (BNT).
- Identifying Applicable Privacy Compliance Documentation.
- Information Sharing to Respond to a Breach.
- Reporting Requirements.
- Assessing and Mitigating the Risk of Harm to Individuals Potentially Affected by the Breach.
- Notifying Individuals Potentially Affected by the Breach.

Contributors to the breach response plan are defined later in this procedure, as well as all other participants in the process.

The BET EX is responsible for advising the SAOP on effectively and efficiently responding to a breach. When designating Agency officials to serve on the Agency's BET EX, the decision maker shall consider the skills and expertise that may be required to respond to a breach effectively and efficiently. In the course of advising the SAOP, the BET EX will consult with the appropriate personnel, who may include:

- Budget and procurement personnel who can provide expertise when a breach involves contractors or an acquisition, or who may help procure services such as computer forensics, cybersecurity experts, services or call center support.
- Human resources personnel who may assist when employee misconduct results in a breach or when an employee is suspected of intentionally causing a breach or violating Agency policy.

[1] A breach response plan is a formal document that includes the Agency's policies and procedures for reporting, investigating and managing a breach. It should be specifically tailored to the Agency and address the Agency's missions, size, structure and functions.

[2] See National Institute of Standards and Technology, Computer Security Incident Handling Guide, Special Publication 800-61 Rev 2, (Aug. 2012).

- Law enforcement personnel who may assist when a breach involves the violation or suspected violation of law or when a breach is the subject of a law enforcement investigation.
- Physical security personnel who may investigate when a breach involves unauthorized physical access to a facility or when additional information regarding physical access to a facility is required.
- Other Agency personnel who may be necessary per specific Agency missions, authorities, circumstances and identified risks.

The BET EX will also complete the following activities:

- Determine whether the Agency's response can be conducted at the staff level or whether the agency must convene the BNT.
- At a minimum, the BNT shall always be convened when a breach constitutes a major incident, as defined below.
- Reassess the Agency's breach response plan at least annually to confirm that the plan is current, accurate and reflects any changes in law, guidance, standards, EPA policy, procedures, staffing and/or technology.
- Document the date of the most recent breach response plan review and submit the updated version of the plan to OMB, when requested as part of annual Federal Information Security Modernization Act (FISMA) reporting.
- Review the fiscal year-end Security Operations Center (SOC) reports, detailing the status of each breach reported and consider whether the Agency should undertake any of the following actions:
    - Update the breach response plan, reflecting all changes in law, guidance, policies, procedures and standards.
    - Develop, revise or implement new policies to protect the EPA's PII holdings.
    - Improve training and awareness.
    - Modify information sharing agreements.
    - Update documentation such as System of Records Notices (SORN), Privacy Impact Assessments (PIA) or privacy policies.

B. Responding to a Breach

All Employees, Grantees and Contractor's Response Activities

All EPA employees, contractors and grantees performing work on behalf of the Agency shall:

- Immediately report any suspected or known breach of PII on Agency systems or systems operated on behalf of the Agency. This includes reporting that laptops, mobile phones, or other devices that may contain PII are believed to be lost, stolen, or otherwise missing. A breach can occur verbally as well as through electronic, paper, or other media.
- Report the suspected or known incident to the EPA Call Center (1-866-411-4372, Option 1).

- Complete the Breach Reporting Form (Appendix B) provided by the EPA Call Center and return it to the Call Center.
  a. Details of the Incident may also be provided to the EPA Call Center to complete the form during the initial call.

EPA Call Center Response Activities

The EPA Call Center shall:
Provide the Breach Reporting Form to the individual reporting the suspected breach and forwards the completed form to the Computer Security Incident Response Center (CSIRC).

Details of the Incident may also be provided to the EPA Call Center to complete the form during the initial call.

CSIRC Breach Response Activities

The CSIRC shall:

- Receive the completed Breach Reporting Form from the EPA Call Center. If the form is incomplete or the CSIRC determines additional information is needed, the CSIRC will contact the individual reporting the suspected or confirmed breach to complete the form or additional information required.
- Evaluate the Breach Reporting Form to determine if the incident involves a possible criminal violation and/or PII.
  - If the incident involves a possible criminal violation, CSIRC will immediately notify offices such as the EPA's Office of Inspector General (OIG), Office of General Counsel (OGC) and Physical Security Office; federal, state or local law enforcement, including local police departments; Federal Protective Service (FPS); or the Federal Bureau of Investigation (FBI).
- Assess whether a breach constitutes a major incident. Factors to be considered include the following:
  - Involves information that is Controlled Unclassified Information.
  - Is not recoverable within a specified amount of time or is recoverable only with supplemental resources.
  - Has a high or medium functional impact on the mission of the Agency.
  - Involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems.
- Report all incidents to the United States Computer Emergency Readiness Team (US-CERT) through the Department of Homeland Security (DHS) US-CERT Incident Reporting System within one hour of discovery or shall update the DHS US-CERT Incident Reporting System within one hour of determining that an already-reported incident has been deemed a major incident. DHS will notify OMB within one hour of the EPA alerting them of the major incident occurrence.
- Collect information regarding major incidents reported to DHS US-CERT, including:
  - A description of each major incident, including:

        - Threats and threat actors, vulnerabilities and impacts.
        - Risk assessments conducted on the information system before the date of the major incident.
        - The status of compliance of the affected information system with security requirements at the time of the major incident.
        - The detection, response and remediation actions the Agency has completed.
    - The number of individuals whose information was affected by the major incident.
    - A description of the information that was compromised.
    - The number of PII incidents reported to DHS US-CERT within the fiscal year.
    - Any major trends continuing from previous years.
- Work with the BET and others, when directed, to determine if the breach incident involves SPII.
    - If SPII is involved, CSIRC will report the major incident to the US-CERT within one hour of discovery and immediately forward the incident report to the BET. CSIRC may be requested to obtain additional information on behalf of the BET or BET EX.
    - If Non-sensitive PII is involved, CSIRC will forward reports directly to the BET for investigation.

BET Breach Response Activities

The BET is chaired by the Agency Privacy Officer (APO) in OMS, Office of Information Security and Privacy (OISP) and co-chaired by the OISP Deputy Director. The chair(s) may work to identify alternate members as practical and appropriate when chair(s) are affected by a breach. A Responsible Organization (RO) is the office where the breach occurred. The RO's Information Security Officer (ISO) serves as the information owner and is notified by the EPA Call Center when the breach is reported. The ISO will assist the BET Response Teams with mitigating the incident as appropriate. Liaison Privacy Official(s) (LPO) and others may be needed as subject matter experts to respond to the breach and will serve in a consultative role.

The BET's primary role is fact-finding. It uses a risk assessment tool to evaluate the vulnerability, threat and likelihood of harm to individuals or organizations after the occurrence of a breach.

If non-sensitive PII is breached, the BET will take the following actions:

- The BET will review the incident report submitted by CSIRC and ensure it provides sufficient information to evaluate the likelihood of risk of harm to the affected 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 Division Director or equivalent of the RO.
- The BET will issue its decision to the RO within 30 calendar days and without unreasonable delay.

- When the BET determines that notification to affected individuals may be warranted, it will forward its findings and recommendations report to the BET EX. The BET EX and the BNT have authority to decide whether to notify affected individuals. In addition, the RO may at its discretion, notify the affected individual(s) within their purview; even if notification isn't recommended by the BET EX or BNT.

The BET will consider a range of recommendations depending on the level of risk:

- Low risk: Privacy training, instructions for EPA staff and others, and notification to management to consider taking appropriate disciplinary action against the person(s) responsible for the breach, if warranted.
- Moderate risk: Privacy training, notification to affected individual(s), and notification to management to consider taking appropriate disciplinary action against the person(s) responsible for the breach, if warranted.
- High risk: Credit monitoring, privacy training, notification to affected individual(s), and notification to management to consider taking appropriate disciplinary action against the person(s) responsible for the breach, if warranted.

If Sensitive PII is breached, the BET will take the following actions:

- The BET will review the incident report submitted by CSIRC and ensure it provides sufficient information 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 BET EX, including whether the risk can be mitigated, whether the individual(s) should be notified, whether credit monitoring should be offered, or whether management should receive notice requesting that they consider taking appropriate disciplinary action against the person(s) responsible for the breach, if warranted.
- The BET will issue its findings and recommendations report to the BET EX within 30 calendar days and without unreasonable delay after receiving the incident report from CSIRC.

BET EX Breach Response Activities

The BET EX decides how the Agency will respond to breaches of SPII, including whether to issue a notification to affected individuals, offer credit monitoring and/or if conduct and discipline actions are warranted.

The BET EX is chaired by the Chief Privacy Officer (CPO), OISP and co-chaired by the Associate General Counsel, Office of General Counsel (OGC). The BET EX may consult additional subject matter experts. The chair(s) may identify alternate members as practical and appropriate when the chairs(s) are affected by a breach.

The BET EX shall complete the following actions:

- Review the BET's report and background documents to determine the necessary course of action. 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 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.
- Prepare a decision memorandum issued to the Office Director of the RO in writing within 30 calendar days and without unreasonable delay after receiving the BET report. The memorandum will include the BET EX's findings and recommendations.

- The BET EX can, at their discretion, refer any incident to the BNT for final Agency decision.

- The BET EX will review and transfer all major incidents to the BNT for final Agency decision.

C. Assessing the Risk of Harm to Individuals Potentially Affected by a Breach

In cases where the BET EX has determined the impact of the incident rises to the level of SAOP involvement, the SAOP, in coordination with the BET and BET EX, shall conduct and document an assessment of the risk of harm to individuals potentially affected by a breach to properly escalate and tailor breach response activities.

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 tool based on guidelines published by the National Institute of Standards and Technology (NIST)-800-12 rev 1 to assess the likelihood of harm to individuals or organizations following breaches of PII. 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., SPII, non-SPII and aggregate PII elements).
- Likelihood the information is readily accessible and usable (e.g., encrypted, unencrypted, paper and password protected).
- Ability of the Agency to mitigate the risk of harm (e.g., Internet vs. Intranet exposure).
- Number of individuals affected, which influences the risk response and method of notification.

In addition to the BET findings and recommendations, the BET EX shall consider the potential harm that could result from the loss or compromise of PII when assessing the risk of harm to individuals potentially affected by a breach. The BET EX shall protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained", in accordance with the Privacy Act. These may include the following:

- A breach of confidentiality or fiduciary responsibility.
- The potential for blackmail.
- The disclosure of private facts.
- Mental pain and emotional distress.
- Financial harm.
- The disclosure of contact information for victims of abuse.
- The potential for secondary uses of the information which could result in fear or uncertainty.
- The unwarranted exposure leading to humiliation or loss of self-esteem.

The BET EX shall consider all risks relevant to the breach, which may include risks to the Agency, Agency information systems, Agency programs and operations, the federal government or national security. These additional risks may properly influence an Agency's overall response to a breach and the steps the Agency should take to notify individuals.

Nature and Sensitivity of the PII Potentially Compromised by the Breach

In addition to the BET findings, the BET EX shall consider the following when assessing the nature and sensitivity of PII potentially compromised by a breach:

- Data Elements
- Context
- Private Information
- Vulnerable Populations
- Permanence

Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual. These data elements include, but are not limited to, social security numbers, passport numbers, bank account numbers, passwords, medical information and biometric identifiers. The BET EX shall also evaluate the sensitivity of all the data elements together:

- Consider the context including the purpose for which the PII was collected, maintained and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individuals.
- Evaluate the extent to which the PII constitutes information that an individual would generally keep private. Such private information may not present a risk of identity theft or other criminal conduct but may pose a risk of harm such as embarrassment, blackmail or emotional distress.
- Consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. When a breach potentially affects a vulnerable population, the Agency may need to provide a different type of notification to that population, provide a notification when it would not otherwise be necessary or provide a notification to individuals other than those whose PII was potentially compromised.
- Consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility

as it ages, while other information is likely to apply to an individual throughout a lifetime.

Likelihood of Access and Use of PII

- Evaluate the likelihood of access and use of encrypted PII, by confirming:
  - Whether encryption[3] was in effect.
  - The degree of encryption.
  - At which level the encryption[4] was applied and whether decryption keys[5] were controlled, managed and used.
- Consider if the PII potentially compromised by a breach also may be rendered partially or completely inaccessible by security safeguards other than encryption. This may include redaction, data masking and remote wiping[6] of a connected device. Physical security safeguards such as a locked case securing documents or devices may also reduce the likelihood of access and use of PII.
- Consider the amount of time that the PII was exposed (i.e., duration of exposure). PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized users.
- Determine whether there is evidence of misuse. In some situations, an Agency may be able to determine with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific breach or that the PII is appearing in unauthorized external contexts.

Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach

The BET, in coordination with the BET EX, shall consider how best to mitigate the identified risks:

- Consider the assessed risk of harm and the circumstances of the breach when deciding whether to offer guidance or provide services to individuals.
- Make final decisions regarding whether to offer guidance or provide services to individuals potentially affected by a breach.

[3]Federal agencies are required to use a NIST-validated encryption method. The SAOP shall consult with the Agency's CISO and other technical experts, as appropriate, to ascertain whether information was properly encrypted. For additional information, refer to National Institute of Standards and Technology Federal Information Processing Standards Publication 140, Security Requirements for Cryptographic Modules at: http://csrc.nist.gov/publications.

[4]There are many ways to encrypt information and different technologies provide varying degrees of protection. Encryption can be applied at the device-level or file-level and to information at rest or in transmission

[5] The protection provided by encryption may be undermined if keys, credentials or authenticators used to access encrypted information are compromised.

[6] See National Institute of Standards and Technology, Guidelines for Managing the Security of Mobile Devices in the Enterprise, Special Publication 800-124 Rev. 1 (June 2013)

- Determine and document the actions that the Agency will take to mitigate the risk of harm. These actions can include countermeasures, guidance or services.
- Advise the RO on whether to take countermeasures, offer guidance or provide services to individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether to offer guidance or provide services to individuals will depend on the circumstances of the breach.

BNT Breach Response Activities

The SAOP convenes and chairs the BNT. The OMS Principal Deputy Assistant Administrator (PDAA) chairs the BNT in the absence of the SAOP. The chair may identify alternate members as practical and appropriate when a member of the BNT is affected by a breach. The BNT is the Agency's core management group.[7]

BNT members consist of senior Agency officials from across the EPA who aid in the coordination of the response, including the following people/offices or their designee:

- The SAOP
- The Chief Privacy Officer (CPO)
- Office of General Counsel
- Legislative affairs official
- Communications official
- Budget personnel
- Procurement personnel
- Human Resources
- Inspector General
- Physical Security
- Responsible Organization

The BNT shall convene only when:

- An incident is referred by the BET EX for a final Agency decision.
- A RO appeals the decision of the BET EX to the SAOP.
- There is a major incident.
- At the discretion of the SAOP or the OEI PDAA as necessary to address incidents with broad impact.

The SAOP shall make final decisions after receiving input from BNT members and shall communicate decisions in writing within 30 calendar days and without unreasonable delay after receiving the BET EX report.

[7] Defined by OMB in Memorandum M-07-16. The core members of the BNT consist of: Senior Agency Official Privacy; Inspector General; General Counsel; Director, Office of Public Affairs; Chief Privacy Officer; Deputy Associate Administrator, Office of Congressional Affairs; Deputy Assistant Administrator, Office of Administration & Resources Management; Chief Financial Officer; Senior Official from Responsible Organization.

RO Breach Response Activities

A RO, in coordination with the BET, BET EX, BNT, EPA Call Center, CSIRC and others involved in breach response activities, shall:

- Take all necessary steps to contain, control and mitigate the risks from the breach and prevent further unauthorized access to or use of PII.
- Manage notification activities; conduct any necessary and appropriate follow-up; implement remedial actions; ensure that appropriate safeguards are in place; provide credit monitoring; and/or notify management to request that they consider taking appropriate disciplinary action against the person(s) responsible for the breach, if warranted.
- Participate in BET, BET EX and BNT meetings to answer questions and provide additional information to aid in decision making.
- Implement all recommendations received from the BET, BET EX or BNT. The BET EX and BNT will determine whether the RO will provide notification, credit monitoring and/or other services.
  - If the RO disagrees with the findings and recommendations, it must appeal the decision within ten working days, as described below.
  - A RO may, at its discretion, notify the affected individual within their purview, even if the BET EX or BNT doesn't recommend notification.
- As appropriate, provide and pay for notification expenditures, including credit monitoring services, within 30 calendar days and without unreasonable delay after receiving the Agency's decision.
- As appropriate, arrange to provide credit monitoring services within 30 calendar days without unreasonable delay with the exception of extraordinary cases that include situations in which the need for 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.
- 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 Privacy Officer (APO).
- Ensure files will be maintained and disposed of in accordance with the Federal Records Act and applicable Agency records control schedule(s).
- Work with OGC and public relations staff when necessary and/or appropriate, to review notification messages before they are released.

Countermeasures

The RO, in coordination with the appropriate EPA organizations, shall 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 the following:

- Monitoring and possibly freezing or closing affected accounts.
- Modifying computer access controls or physical access controls.
- Taking other necessary and appropriate actions.

These steps will be taken without undue delay and be consistent with current requirements under the NIST, the Federal Information Processing Standards (FIPS) and OMB Directives and Agency policies.

Appealing Agency Decisions

A RO may appeal decisions issued by the BET or BET EX, as described below.

Appealing a BET Recommendations

If a RO does not agree with a recommendation issued by the BET, it may appeal the decision to the BET EX within 10 calendar days after receipt and provide an explanation for the disagreement.

The BET EX shall issue a recommendation to a RO within 10 calendar days. The decision issued by the BET EX is the Agency's final decision.

Appealing a BET EX Recommendations

If a RO does not agree with a recommendation issued by the BET EX, it may appeal the decision to the SAOP within 10 calendar days after receipt. The appeal must be in writing and provide an explanation for the disagreement.

The SAOP shall convene the BNT within 15 calendar days and without unreasonable delay after the appeal is received.

The BNT shall issue a recommendation to the RO within 30 calendar days and without unreasonable delay. The recommendations issued by the BNT is the Agency's final decision when BET EX decisions are appealed.

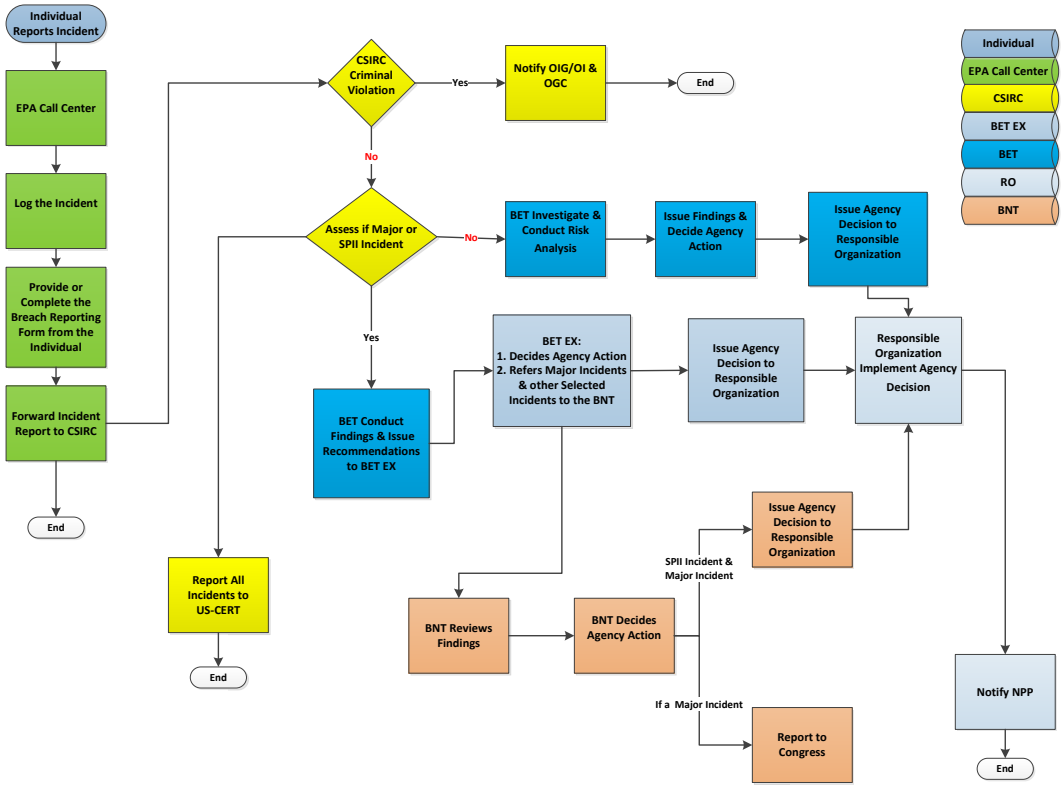
Appealing a BNT Recommendations

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

The SAOP shall notify the Deputy Administrator when ROs are non-compliant or do not respond to Agency recommendations within 30 calendar days.

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Figure 1. Breach Response Process Flow



D. Other Third Party Notifications and Requirements for Breach Response

When the Agency decides that notice to third parties is required, the timing, order and content of the notice will be carefully coordinated with appropriate organizations (e.g., OGC, OMS, 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:

- US-CERT
- Law Enforcement, the Inspector General and General Counsel
- Congress
- Attorney General
- Financial institutions
- Media
- Public

Contracts and Contractor Requirements for Breach Response

The Chief Acquisition Officer (CAO), in coordination with the SAOP, should ensure that contract provisions to assist with the response to a breach are uniform and consistently included in Agency contracts. Additionally, the CAO and SAOP should:

- Ensure that contract terms necessary for the Agency to respond to a breach are included in contracts when a contractor collects or maintains federal information on behalf of the Agency or uses or operates an information system on behalf of the Agency.
- Ensure other agreements e.g. Cooperative, Inter-Agency, or Memorandum of Understanding include the appropriate language that allows for sharing and protecting of PII and/or the provisions that require reporting and managing a suspected or confirmed breach of PII.
- Require contractors to cooperate with and exchange information with Agency officials, as determined necessary by the Agency, to effectively report and manage a suspected or confirmed breach.
- Require contractors and subcontractors (at any tier) to properly encrypt SPII in accordance with applicable policies and to comply with any Agency-specific policies for protecting SPII.
- Require regular training for contractors and subcontractors (at any tier) on how to identify and report a breach.
- Require contractors and subcontractors (at any tier) to report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the Agency's incident management policy and US-CERT notification guidelines.
- Require contractors and subcontractors (at any tier) to maintain capabilities to determine what federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access federal information, and identify the initial attack vector.
- Allow for an inspection, investigation, forensic analysis and any other action necessary to assist with responding to a breach and to ensure compliance with Agency policies, the Agency's breach response plan.
- Identify roles and responsibilities in accordance with this procedure and the Agency's breach response plan.
- Explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

The SAOP shall ensure that the Agency's breach response plan and system security authorization documentation clearly defines the roles and responsibilities of contractors that operate federal information systems that create, collect, use, process, store, maintain, disseminate, disclose or dispose of PII on behalf of the Agency. Any such roles and responsibilities should be further defined in the contract to ensure contractor compliance with the EPA's requirements.

- When a contractor provides notification on behalf of the EPA, such activities shall be in accordance with OMB guidance and the EPA's breach response plan and shall be coordinated with and subject to prior written approval by the SAOP.
- The Agency may require the contractor to take countermeasures to mitigate the risk of harm to potentially affected individuals or to protect PII on behalf of the Agency, including operating call centers and providing resources for potentially affected individuals.

Any required countermeasures must be consistent with OMB Memorandum M-16-14, which, except under limited circumstances, requires the use of General Services Administration's (GSA) Identity Protection Services (IPS) Blanket Purchase Agreements (BPAs). GSA has awarded government-wide Federal Supply Schedule BPAs for identity monitoring, credit monitoring and other related services[8].

The Federal Acquisition Regulatory (FAR) Council, in coordination with OMB, shall work promptly to create appropriate contract clauses and regulatory coverage to address contractor requirements for breach response in the FAR. In developing regulatory amendments, the FAR Council shall consult with the Federal Privacy Council and the Federal CIO Council, as appropriate.

Office of Mission Support Requirements for Breach Response

The EPA physical security personnel, shall contain, control and prevent further unauthorized access in the event that any incident involves a physical security breach affecting PII.

- At EPA Headquarters, this responsibility falls under OMS. The responsibility may reside with other organizations in EPA regional offices.
- Steps may include changing locks or key codes, securing/locking file cabinets, deactivating identification cards, adding further physical security to entrances and exits, alerting the Federal Protective Service and developing special instructions, as appropriate.

OMS is a delegated authority by the SAOP to directly respond to incidents involving the misfiling of PII in electronic official personnel files (e-OPFs). OMS will complete the following actions:

- Notify employees when their PII is misfiled without BET review.
- Provide the APO the number of misfiling's e-OPF 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.

[8] GSA Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) includes 132-45B: Incident Response Services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their IT systems and restore their networks to a more secure state.

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Grants and Grantee Requirements for Breach Response

The EPA shall ensure that grant recipients who use or operate a federal information system or creates, collects, uses, processes, stores, maintains, disseminates, discloses or disposes of PII within the scope of a federal award have procedures in place to respond to a breach and include terms and conditions requiring the recipient to notify the federal awarding Agency in the event of a breach. The procedures should promote cooperation and the free exchange of information with federal awarding Agency officials, as needed, to properly escalate, refer and respond to a breach.

Law Enforcement, Inspector General and General Counsel Requirements for Breach Response

The CSIRC shall complete the following:

- Identify the Agency officials responsible for notifying and consulting with law enforcement and Offices of Inspectors General and General Counsel on behalf of the Agency.
- Ensure that, when a breach warrants a report to law enforcement,[9] the report occurs promptly even if the breach is unconfirmed or the circumstances are still unclear.
- Coordinate with the identified Agency officials to ensure that law enforcement and Offices of Inspectors General and General Counsel receive timely notification when appropriate.
- Consider and advise appropriate officials on whether the specific circumstances and type of PII potentially compromised by a breach require the involvement of other oversight entities.

Congressional Requirements for Breach Response and Major Incidents

The CSIRC shall notify the SAOP when an issue arises that may require communications with congressional committees[10]. The SAOP will contact the Director of the Office of Congressional and Intergovernmental Relations (OCIR) when necessary.

The OCIR Director, in consultation with the SAOP, shall coordinate all communications and meetings with congressional committees. The OCIR Director will notify Congress within seven days of the date on which there is a reasonable basis to conclude that a breach that constitutes a major incident has occurred.

[9]Such offices include the EPA's Office of Inspector General (OIG); the Office of General Counsel (OGC), EPA Security Office; federal, state or local law enforcement, including local police departments; the Federal Protective Service (FPS); and/or the Federal Bureau of Investigation

[10] The Committee on Government Reform; the Committee on Homeland Security; the Committee on Science of the House of Representatives; the Committee on Homeland Security and Governmental Affairs; the Committee on Commerce, Science and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; and the Comptroller General.
See: 44 U.S.C 3554 (b)(7)(C)(III) (aa)-(bb).

The SAOP shall supplement the initial seven-day notification to Congress with a report no later than 30 days after the Agency discovers the breach. This supplemental report must include the following:

- A summary of information available about the breach, including how the breach occurred.
- An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals.
- A description of any circumstances necessitating a delay in providing notice to affected individuals.
- An estimate of whether and when the Agency will provide notice to affected individuals.

Reporting to the Attorney General

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.

Reporting to Financial Institutions

The Office of the Chief Financial Officer (OCFO) shall 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 aforementioned steps.

Reporting to the Media and the Public

The Director of the Office of Public Affairs (OPA), in coordination with the RO and OMS, shall communicate with the media and the public.

E. Identifying Logistical and Technical Support to Respond to a Breach

The SAOP should identify the logistical capabilities that exist within the Agency and which offices are responsible for maintaining those capabilities. The SAOP should understand the ability of the Agency to support any resource-intensive activities that may be necessary to provide notification, offer guidance and provide services to individuals potentially affected by a breach, such as call center services, updating websites and providing translation services.

As a part of this process, the CIO may identify gaps in the Agency's technical capabilities and therefore should communicate with the CAO and other Agency officials on the need to enter into contracts or to explore other options for ensuring that certain functions are immediately available during a time-sensitive response.

F. Identifying Applicable Privacy Compliance Documentation

The SAOP shall identify all the applicable privacy compliance documentation when responding to a breach:

- Which SORNs, PIAs and privacy notices apply to the potentially compromised information?
- Is PII maintained as part of a system of records that needs to be disclosed as part of the breach response? Is the disclosure permissible under the Privacy Act? How will the Agency account for the disclosure?
- If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, does that information require new or revised SORNs or PIAs?
- Are the relevant SORNs, PIAs and privacy notices accurate and up-to-date?

The compliance documentation will help identify what information was potentially compromised and the population of individuals potentially affected, as well as the purpose for which the information had originally been collected, the permitted uses and disclosures of the information, and other information that may be useful when developing the Agency's response.

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

The EPA shall complete the following:

- Establish rules of behavior, including consequences for violating such rules, for employees, contractors and others who have access to federal information or information systems.
- Include in the rules of behavior the consequences for failing to comply with the reporting requirements in this procedure.
- Ensure that employees and contractors have read and agreed to abide by the rules of behavior for the federal information and information systems for which they require access prior to being granted access.

G. Privacy Act Routine Uses Required to Respond to a Breach

The SAOP shall ensure that all the EPA's Privacy Act SORNs include routine uses for the disclosure of information necessary to respond to a breach either of the EPA's PII or, as appropriate, to assist another Agency in its response to a breach.[11]

[11] 5 U.S.C. 552a(b)(3). The publication of appropriate routine uses is required under the Privacy Act and thus would be necessary in order to disclose information for the purpose of executing an Agency's obligations to effectively manage and report a breach under FISMA. Disclosures pursuant to a routine use are permissive, not mandatory. See Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9,1975), available at http://www.whitehouse.gov/sites/default/filesomb/assets/omb/inforegimp Implementation _guidelines.pdf.

Notification Guidance

The BET EX shall determine how to mitigate the risk of harm to individuals potentially affected by a breach by considering what guidance to provide to those individuals regarding how they may mitigate their own risk of harm. The BET EX will use the information available at www.IdentityTheft.gov/databreach as the baseline when drafting guidance. The Federal Trade Commission (FTC) provides specific guidance for when a breach involves SSNs, charge card information, bank accounts, driver's licenses, children's information and account credentials. Additionally, the BET EX may advise individuals to change passwords and encourage the use of multi-factor authentication for account access.

Services

The BET EX shall determine if there are services[12] the Agency can provide when determining how to mitigate the risk of harm to individuals potentially affected by a breach. The BET EX shall identify those services which best mitigate the specific risk of harm resulting from the breach. Services may include but are not limited to:

- Use the GSA BPAs in accordance with OMB Memorandum M-16-14 when choosing identity monitoring, credit monitoring and other related services to mitigate the risk of harm to individuals potentially affected by a breach.
- Consider the services included in Appendix C of this procedure, as well as additional services available in the future.
- When the EPA determines that credit monitoring is warranted, it will be provided to any affected individuals for at least one year free of charge, if not covered by an existing agreement. Affected individuals must notify the EPA, as defined in the notification letter, that credit monitoring is requested.
- 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. The 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

H. Notifying Individuals Potentially Affected by a Breach

The BET EX and/or BNT may review the BET's risk assessment to make 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

[12] Many of the services currently available in today's marketplace only mitigate risks of financial identify theft. Even the most comprehensive services are unable to mitigate the potential harms resulting from the evolving threat and risk landscape.

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.

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. Because each breach is fact-specific, the decision of whether to notify individuals will depend on the circumstances of the breach.[13] A RO, at their discretion, can choose to notify an individual within their purview, even if the recommendation isn't suggested by the BET EX.

Source of the Notification

The RO Office Director or an individual from the RO with equivalent authority shall notify affected individuals in writing when notification is necessary, helpful or otherwise required.

Notification letters must be approved based on type of method used and signed by an Office Director or higher authority with a copy to the APO. 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 sign the notifications to the individuals affected by the breach.

Timeliness of the Notification

The RO shall provide notification within 30 calendar days and without unreasonable delay when it is determined that disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information system or the integrity of an investigation.

Content of the Notification

The RO shall provide written notice to the affected individuals, including 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 (e.g., full name, SSN, date of birth, home address, account number and disability code).
- A statement of whether the information was encrypted or protected by other means when it is determined that disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information system.

[13] The Agency's decision to offer guidance, take countermeasures, or provide services to individuals potentially affected by a breach may not necessarily notify those individuals both of the breach and of those steps taken to mitigate any identified risks. However, the EPA may also choose to notify individuals even when the Agency is not providing a specific service.

- Guidance to potentially affected individuals on how they can mitigate their own risk of harm, countermeasures the Agency is taking and services the Agency is providing to potentially affected individuals, if any.
- Steps the Agency is taking, if any, to investigate the breach, to mitigate losses and to protect against a future breach.
- Point of contact for individuals [14]requiring more information, including a telephone number (preferably toll-free), email address and postal address.

Method of Notification

The RO shall select the method for providing notification. The best method for providing notification will potentially depend on the number of individuals affected, the available contact information for the potentially affected individuals and the urgency with which the individuals need to receive the notification.

- First-Class Mail: First-class mail notification to the last known mailing address of the individual in Agency records should be the primary means by which notification is provided. Where the Agency has reason to believe the address is no longer current, the Agency should take reasonable steps to update the address by consulting with other agencies such as the U.S. Postal Service. The notification should be sent separately from any other mailing so that it is conspicuous to the recipient.
- Email: While email is not recommended as the primary form of notification, in limited circumstances it may appropriate. For example, if the individuals potentially affected by a breach are internal to the Agency, it may be appropriate to use an official email address to notify a small number of employees, contractors, detailees or interns via their official email addresses. ".gov" or ".mil" email may be used to notify an individual on his or her ".gov" or ".mil" email that his or her PII was potentially compromised by a breach.
- 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. Telephone notification, however, should be contemporaneous with written notification by first-class mail.
- Substitute Notification: This type of notice may also be beneficial if the Agency needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly time-sensitive. A substitute notification should consist of a conspicuous posting of the notification on the home page of the Agency's website and/or notification to major print and

[14] The EPA may provide additional details in a Frequently Asked Questions (FAQ) format on the Agency website or via an enclosure. The FAQs on the website may be beneficial because they can be easily updated, contain links to more information, provide more tailored information than the formal notification and can be easily translated into multiple languages. For a breach that potentially affects a large number of individuals, or as otherwise appropriate, the EPA may establish toll-free call centers staffed by trained personnel to handle inquiries from the potentially affected individuals. If the EPA has knowledge that the potentially affected individuals are not English speaking, or require translation services, notification should also be provided in the appropriate languages to the extent feasible. The EPA may seek additional guidance on how to draft a notification from the FTC, which is a leader in providing clear and understandable notifications to consumers, as well as from communication experts.

broadcast media, including major media in areas where the potentially affected individuals reside. Notification to media should include a toll-free phone number and/or an email address that an individual can use to learn whether or not his or her personal information is affected by the breach. In instances where there is an ongoing investigation and the facts and circumstances of a breach are evolving, the EPA can consider whether it is appropriate to establish an ongoing communication method for interested individuals to automatically receive updates.

Special Consideration

There may be instances when the EPA provides notification to individuals other than those whose PII was potentially compromised. For example, when the individual whose information was potentially compromised is a child, the Agency may provide notification to the child's legal guardian(s). Special care may be required to determine the appropriate recipient in these cases.

Give special consideration to providing notice to individuals who are visually or hearing impaired in accordance with Section 508 of the Rehabilitation Act of 1973, as amended. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the Agency website.

Tracking, Documenting and Externally Reporting the Agency's Response to Breaches

The Call Center, CSIRC and BET shall develop and maintain a formal process to track and document each breach reported to the Agency, which ensures that the SAOP is made aware in a timely manner of each report of a suspected or confirmed breach:

- Complete or assign the internal reporting template to the individual reporting the breach (See Appendix B).
- Disclose information to appropriate agencies, entities and persons when it is suspected or confirmed that:
  - The security or confidentiality of information in the system has been compromised.
  - 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.
  - Third parties are necessary to assist in connection with the Agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize or remedy such harm.

The BET shall complete the following:

- Keep the CSIRC informed of the status of an ongoing response and for determining when the response to a breach has concluded.
- Report the conclusion of the Agency's response to a breach to the CSIRC with the outcome of the response.
- Ensure that the process for internally tracking each reported breach allows the Agency to track and monitor the following:

- The total number of breaches reported over a given period of time.
- The status for each reported breach, including whether the Agency's response to a breach is ongoing or has concluded.
- The number of individuals potentially affected by each reported breach.
- The types of information potentially compromised by each reported breach (see Appendix B of this Procedure).
- Whether the Agency, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach.
- Whether the Agency, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach.
- Whether a breach was reported to US-CERT and/or Congress.

I. Lessons Learned

The BET and the BET EX shall complete the following:

- Evaluate the handling and disposition of all suspected or actual breaches reported under these procedures, periodically.
- Determine whether tasks can be conducted more effectively and make modifications to the processes as appropriate.
- Document any changes including challenges in the breach response plan, policies and other documents.

The CSIRC and BET shall provide the SAOP with a detailed report at the end of each quarter of the fiscal year on the status of each breach reported during the fiscal year that remains open or that was closed since the last report.

The SAOP shall complete the following:

- Conduct a review of the report as well as validate the accuracy of the reported breaches.
- Meet with the BNT when the breach is reported to Congress to review Agency's response to the breach and identify any lessons learned.

J. Tabletop Exercises

The SAOP shall convene the breach response teams to hold a tabletop exercise[15] at least annually.

[15] The purpose of the tabletop exercise is to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand their specific roles. Testing breach response plans is an essential part of risk management and breach response preparation. Tabletop exercises should be used to practice a coordinated response to a breach, to further refine and validate the breach response plan and to identify potential weaknesses in an Agency's response capabilities.

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

7. ROLES AND RESPONSIBILITIES

Administrator

- Ensures that the EPA's privacy interests are protected and that PII is managed responsibly within the Agency.
- Designates SAOP, who has Agency-wide responsibility and accountability for the Agency's Privacy Program.

Agency Employees, Grantees and Contractors

- Report suspected or known breaches of PII immediately to the Primary ISO and the EPA Call Center at 1-866-411-4372, Option 1 as soon as the breach is suspected or confirmed.
- Encrypt all SPII in transmission.
- Double wrap all SPII in transport.
- Comply with the provisions of the Privacy Act and Agency regulations and policies pertaining to collecting, accessing, using, disseminating and storing PII and Privacy Act information.
- Ensure that PII contained in a system of records to which they have access in the performance of their duties is protected so that the security and confidentiality of the information are preserved.
- Not disclose any personal information contained in any system of records or PII collection, except as authorized.
- Access and use only information for which they have official authorization.
- Be accountable for their actions and responsibilities related to the information and resources entrusted to them.
- Protect PII from disclosure to unauthorized individuals.
- Protect the integrity of PII in their possession.
- Protect the availability of information and ensure appropriate access levels.
- Be knowledgeable of PII and Privacy Act policies, requirements and issues.
- Adhere to privacy rules of conduct and may be subject to all applicable penalties under the Privacy Act. Each case will be handled on an individual basis with a full review of all pertinent facts.
- Be subject to disciplinary action for failure to take appropriate action upon discovering a breach or for failure to take required steps to prevent a breach from occurring or re-occurring.

Agency Privacy Officer (APO)

- 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 ROs, as appropriate.

Breach Evaluation Team (BET)

- Decides how the Agency will respond to incidents involving non-sensitive PII.

- Makes recommendations and/or mandatory requirements to the Breach Evaluation Team Executive Committee when sensitive PII is involved.

Breach Evaluation Team Executive Committee (BET EX)

- Determines what level of mitigating factors is required and/or commensurate with the type of breach.
- Decides how the Agency will respond to breaches of sensitive PII.
- Notifies management to request that they consider taking appropriate disciplinary action against person(s) responsible for the breach, if warranted.
- Establishes whether credit monitoring and/or other services will be offered to the affected individuals.

Breach Notification Team (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 RO.
- Responds to breaches of major incidents.

Computer Security Incident Response Capability (CSIRC) Team

- Provides incident management support to the Agency.
- Reports breaches of sensitive PII to the DHS US-CERT.
- Forwards all breaches of PII to the BET.
- Works with BET in instances where there is an electronic breach.
- Works with BET, BET EX, BNT, and SAOP if necessary.
- Reports major incidents to Congress.

Contractors

- Report 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).
- Inform the Contracting Officer (CO) or Contracting Officer Technical Representative (COTR) after reporting the incident to the CSIRC.

Chief Privacy Officer (CPO)

- 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.
- Serves as a co-chair of the BET EX.
- Participates on the BNT.
- Advises the SAOP on privacy issues.

Deputy Administrator

- Issues final Agency decisions when the SAOP presents referrals of willful inaction by the RO.

Principal Deputy Assistant Administrator (PDAA), Office of Mission Support (OMS)

- Chairs the BNT when the SAOP is absent.

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)

- Implements information management functions, including privacy requirements, in their organizations.
- Serves as the organizational point of contact for the Agency Privacy Officer.

Information Owner (IO)

- 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.
- 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.

Information Security Officer (ISO)

- Ensures information security in their organizations.
- Works with CSIRC and the BET to address PII incidents involving electronic systems under their purview.
- Assists Office Director in complying with recommendations issued by BET, BET EX or BNT.

Information System Owner (IS)

- Responsible for the overall procurement, development, integration, modification or operation and maintenance of the information system.
- 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.
- Assists in the identification, implementation and assessment of the common security controls.

Liaison Privacy Official (LPO)

- Administers the day-to-day privacy activities in their programs and regions.
- Assists with breaches and is the primary point of contact for the National Liaison Privacy Official.
- Assists the Office Director in complying with recommendations issued by BET, BET EX or BNT.

Office of Mission Support (OMS)

- Responds to incidents involving the misfiling of PII in electronic official personnel files (e-OPFs) without BET review.
- Is responsible for the physical security of the EPA's buildings and providing contact information, when required, to locate employees who are affected by the breach. OARM is a core member of the BNT.
- Ensure contractors are aware of their responsibility to report all suspected or confirmed breaches of PII and assist in mitigating the incident.

Office of Congressional and Intergovernmental Relations (OCIR)

- Coordinates all communications and meetings with congressional committees and members of Congress.

Office of General Counsel (OGC)

- Provides legal support and guidance in responding to a suspected or known breach.
- Serves as co-chair of the BET EX.
- Participates on the BNT.

Office of Inspector General (OIG)

- Assists CSIRC with its investigation when needed.
- Conducts evaluations 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 Public Affairs (OPA)

- Advises OMS concerning external notifications, including the strategy for notifying the media and posting information to OMS's homepage, as appropriate.
- A senior official from the OPA is a core member of the BNT.

Office of Regional Counsel (ORC)

- Provides legal support and guidance in responding to a suspected breach when it occurs in an EPA regional office.
- Participates in BET EX and/or BNT meetings, as required.

Office of Information Technology Operations (OITO)

- Ensures 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 (RO)

- The office where the information was comprised.

- Implements and provides the resources to support the Agency's decision regarding breach response activities.
- Responds to recommendations issued from BET, BET EX or BNT.
- Pays for credit monitoring or other services dictated by recommendations issued from BET, BET EX and BNT.

Senior Agency Official for Privacy (SAOP)

- Chairs the BNT and convenes meetings, as appropriate.
- 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.
- Makes risk-based decisions on when a SORN is required and/or the approach taken when a breach has occurred from a SORN.
- Verifies 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.
- Makes final decisions on Agency breaches referred from BET EX or an appeal of a BET EX initial recommendation with input from the BNT.
- Appoints the Chief Privacy Officer.

Senior Information Official (SIO)

- Implements Agency privacy regulations, policies and procedures within their respective organizations and protects individuals' privacy by safeguarding PII.

U.S. Computer Emergency Readiness Team (US-CERT)

- Leads efforts to improve the nation's cybersecurity posture, coordinates cyber information sharing and proactively manages cyber risks to the nation while protecting the constitutional rights of Americans.
- Works with CSIRC in instances where there is an electronic breach.

8. RELATED INFORMATION

- EPA Information Security Policy, CIO 2150.3
- EPA Order 1900.1A CHG 2 Interacting with Contractors, December 13, 2005.
- EPA Privacy Policy, CIO Directive 2151, September 14, 2015.
- EPA Role Based and Security Awareness Training.
- EPA CIO 215 0-P-08.2, Information Security – Incident Response Procedures.
- Privacy Policy Protecting SPII-2115-P-10.0.

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.

- **Consequences for non-compliance** - Consequences will be commensurate with the level of responsibility, type of PII involved and the severity of the violation. The circumstances, including whether the behavior or action was intentional, will be considered in taking appropriate action. Any action taken must be consistent with law, regulation, applicable case law and any relevant collective bargaining agreement. Consequences can include suspension of access privileges, reprimand, suspension, demotion, removal and criminal and civil penalties, including prison terms and fines.
- **Harm** - Any adverse 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 imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system or constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies.
- **Major Incident** - Any incident that is likely to result in demonstrable harm to the national security interests, the Agency, foreign relations or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
- **Oral -** Information conveyed verbally.
- **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. PII may be classified into sensitive and non-sensitive.
- **Permanence -** A continued relevance and utility of the PII over time that cannot be replaced or substituted easily.
- **Private Information -** The extent to which PII, in a given context, reveals private and personal information about an individual. Examples of private information include derogatory personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy-related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, immigration status or passwords.
- **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) that contains the individual's name, or any identifying number, or symbol particularly 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.
- **Risk-based Tool - A tool used to** assess the potential risk of harm to affected individuals caused by a breach incident.

- **Sensitive Personally Identifiable Information (SPII)** - Social Security numbers or comparable (e.g., biometrics and passport number), or financial and medical information associated with individuals. Sensitive PII is a subset of PII and requires additional levels of security controls.

Type of Breach

(1) **Intentional Breach**: The SAOP should determine if the target was the information or the device housing the information, such as a mobile phone or laptop. The SAOP should also determine if the compromise of the information was accidental.

(2) **Unintentional Breach**: The risk of harm to individuals may be lower when a breach is unintentional, either by user error or by failure to comply with agency policy. Breach response officials must conduct a case-by-case assessment to determine the risk of harm.
(3) **Unknown**: In many circumstances, the SAOP may be unable to determine whether a breach was intentional or unintentional. In these instances, the SAOP shall consider the possibility that the breach was intentional. The agency may know who received the compromised PII, which could help the SAOP assess the likely risk of harm to individuals. For example, breaches are often reported by recipients who receive information they should not have.

- **Vulnerable Population** - An extent to which a breach of PII disproportionately impacts a disadvantaged population. Potentially vulnerable populations include, but are not limited to, children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence or stalking.

10. WAIVERS

No waivers of the requirements of this procedure will be granted.

11. MATERIAL SUPERSEDED

Procedure for Responding to Breaches of Personally Identifiable Information (PII), CIO P-2151-P-02.2, August 7, 2013.

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

12. CONTACTS

For further information, please contact the Office of Mission Support, Office of Information Security and Privacy (OISP).

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2019.08.27 16:50:24 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Appendix A: Acronyms

APO -	Agency Privacy Officer
BET -	Breach Evaluation Team
BET - EX -	Breach Evaluation Team Executive Committee
BNT -	Breach Notification Team
BRT -	Breach Response Teams (BET, BET EX, and BNT)
BPA -	Blanket Purchase Agreements
CAO -	Chief Acquisition Officer
CIO -	Chief Information Officer
CO -	Contracting Officer
COTR -	Contracting Officer Technical Representative
CPO -	Chief Privacy Officer
CSIRC -	Computer Security Incident Response Capability
CUI -	Controlled Unclassified Information
DAA -	Deputy Assistant Administrator
DCIS -	Deputy Chief Information Security Officer
DHS -	Department of Homeland Security
e-OPF -	Electronic Official Personal Files
EPA -	Environmental Protection Agency
FBI -	Federal Bureau of Investigation
FISMA -	Federal Information Security Modernization Act
FIPS -	Federal Information Processing Standards
FOIA -	Freedom of Information Act
FPS -	Federal Protective Service
IMO -	Information Management Official
IO -	Information Owner
IS -	Information System Owner
ISO -	Information Security Officer
IPS -	Identity Protection Services
GSA -	General Services Administration
LPO -	Liaison Privacy Official
NIST -	National Institute of Standards and Technology
NPP -	National Privacy Program
OARM -	Office of Administration and Resources Management
OMB -	Office of Management and Budget
OCFO -	Office of the Chief Financial Officer
OCIR -	Office of Congressional and Intergovernmental Relations
OMS -	Office of Mission Support
OGC -	Office of General Counsel
OIG/OI -	Office of Inspector General/Office of Investigation
OITO -	Office of Information Technology Operations
OISP -	Office of Information Security and Privacy
ORC -	Office of Regional Counsel
PII -	Personally Identifiable Information
RO -	Responsible Organization
SAOP -	Senior Agency Official for Privacy
SIO -	Senior Information Official

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

SOC -	Security Operation Center
SORN -	System of Records Notices
SSN -	Social Security Number
TDD -	Telecommunications Device for the Deaf
US-CERT -	United States Computer Emergency Readiness Team

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Appendix B: Breach Reporting Template

Breach Reported by:			
Name:	<<First>> <<Last>>	**Office Director:**	<<First> <<Last>>
Email:	<< Official Email >>	**Title:**	<< Official Title >>
Phone:	<< Official Phone >>	**Phone:**	<< Official Phone >>

Summary of the Breach:

Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including:

a. A description of the parties involved in the breach;
b. The physical or electronic storage location of the information at risk;
c. If steps were immediately taken to contain the breach;
d. Whether the breach is an isolated occurrence or a systematic problem;
e. Who identified the breach, if applicable; and
f. Any other pertinent information.

Date and Time of the Breach:	< XX/XX/XXXX, Approximate Time >>
Location of Breach (e.g. lost on a plane, stolen from a car, posted on a website or share drive, etc.)	

Type of Breach:

Lost Information or Equipment	YIN	**Unauthorized Disclosure** (e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, disclosing documents publicly with sensitive information not redacted)	YIN
Stolen Information or Equipment	YIN	**Unauthorized Access** (e.g., an unauthorized employee or contractor accesses information or an information system)	YIN
Unauthorized Equipment (e.g., using an unauthorized personal device, server, or email account to store PII)	YIN	**Unauthorized Use** (e.g., employee with Agency-authorized access to database or file accesses and uses information for personal purposes rather than for official purposes)	YIN

Type of Information breached:

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Specific Information/File Types		
Financial banking Information Check Information Credit History Information	Law Enforcement Information Security Clearance/Background	Security Clearance/Background Check Information

Storage&Medium:			
Laptop or Tablet	YIN	**Smartphone**	YIN
Desktop	YIN	**Paper files**	YIN
External Storage Device	YIN	**External Storage Device** (e.g., CD, DVD, USB Drive, etc.)	YIN
IT System (Intranet/Shared Drive)	YIN	**Oral Disclosure**	YIN
Email:	<< Provide email address and note the Agency, cloud server, personal, private >>		
Other:	<< Provide a detailed description of the medium >>		

Number of individuals and Safeguards	
Number of individuals potentially affected by the breach?	<< ##### >>
Was the information unstructured? (e.g., open fields on a form or survey)	**Y/N**
Was the information encrypted?	<< ##### >>
Does a duplicate set of the potentially compromised information exist?	**Y/N**
Additional Information	
Internal breach (e.g., within the Agency's network), external, both, or unknown?	<< >>
What counter measures, if any, were enabled when the breach occurred?	
<< List all that apply; include whether NIST certified (e.g., hard drive encryption on laptop, encryption of electronic files, password on smartphone recovered and located) >>	
What steps, if any, have already been taken to mitigate potential harm?	
<< e.g., calling or sending separate email(s) to recipient(s) of an unauthorized email to request deletion of original email, contacting web publishing to remove un-redacted documents from public website, etc.>>	
Do you have knowledge that any information involved in the breach was intentionally stolen or misused	Y/N
<< If yes, describe the basis for your knowledge and how the information may have been misused (e.g., evidence of identity theft, hacking, adverse publicity, etc.) >>	

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Medical/Emergency Information (Select all that apply)		
Medical/Health Information	Mental Health Information	Disability Information
Workers' Compensation Information	Patient ID Number	Emergency Contact Information

Responding to Personally Identifiable Information (PII) Breach Procedure		
Directive No.: CIO 2151-P-02.4	CIO Approval: August 2019	Review Date: August 2021

Appendix C: Examples of Guidance an Agency May Offer

Credit Freeze: A credit freeze restricts access to an individual's credit report. When offering this type of guidance, an Agency should be aware that because access to a credit report is usually required by creditors, a credit freeze can prevent creditors from approving a new account.

Credit Freezes and Children: Guardians are sometimes able to place a freeze on a child's credit, even if the child does not yet have a credit history. Several states mandate that all credit bureaus provide this option. Outside those states, the option may still be available depending on the credit bureau. In these instances, guardians may have to provide additional information about themselves as well as the child in order to show the relationship.

Closing or Changing Accounts: Individuals should immediately dispute any unauthorized charges to existing accounts, including closing or changing account numbers so that unauthorized activity does not continue. This will not prevent new unauthorized accounts of which individuals may be unaware.

Obtaining a Free Credit Report: Individuals can obtain a free credit report yearly from each of the three national credit bureaus (Equifax, Experian, and Trans Union) from annualcreditreport.com or by calling the credit reporting agencies' toll-free numbers. Individuals should review their credit reports for any accounts they do not recognize.

Cyber Hygiene: Agencies should also consider providing individuals with resources on good cyber hygiene (e.g., setting up multi-factor authentication, using complex passwords). Resources include: DHS's Stop. Think. Connect. Campaign at: https://www.dhs.gov/stopthinkconnect or https://www.ftc.gov/onguardonline; US-CERT's tips on protecting privacy at: https://www.uscert.gov/ncas/tips/ST04-013; and US-CERT's tips on preventing online identity theft at: https://www.us-cert.gov/ncas/tips/ST05-019.

Fraud Alert: A fraud alert tells creditors that they must take reasonable steps to verify the identity of the individual who is applying for credit. A fraud alert also allows individuals to order one free copy of the individual's credit report from each of the three national credit bureaus. To place this alert, individuals can contact one of the three national credit bureaus, who must then notify the others. The initial fraud alert stays on the credit report for 90 days and can be renewed.

FTC.gov/idtheft: The FTC's website provides free identity theft resources for individuals as well as community leaders, businesses, advocates, and law enforcement to share in their communities. The website includes resources on proactive steps individuals can take to monitor and protect their information and educate themselves on the different types of identity theft and the resources available to protect against and recover from identity theft.

IdentityTheft.gov: This is the Federal Government's one-stop resource for identity theft victims. Individuals can use the website to report identity theft and get a personalized recovery plan that walks them through each step, updates the plan as needed, and pre-fills letters and forms. It also

advises individuals on steps they can take to prevent identity theft when they receive notice that their PII has been compromised. The website is managed by the FTC and is integrated with the FTC's complaint system, which makes the complaint information available to law enforcement across the country through Consumer Sentinel, a secure online database available to law enforcement.