

Office of Government Ethics
BREACH OF PERSONALLY IDENTIFIABLE INFORMATION
NOTIFICATION POLICY AND RESPONSE PLAN

September 2019
Program Counsel Division

**U.S. OFFICE OF GOVERNMENT ETHICS
BREACH OF PERSONALLY IDENTIFIABLE INFORMATION
BREACH NOTIFICATION POLICY AND RESPONSE PLAN**

I. Background

The U.S. Office of Government Ethics (OGE) is committed to protecting the security and integrity of its electronic and physical information systems. It is the responsibility of all OGE employees, OGE contractors, and system users to safeguard all personally identifiable information in OGE's information systems. Because a breach of personally identifiable information (PII) may result in financial loss and personal hardship, it is imperative that OGE protect personally identifiable information in its possession.

The Office of Management and Budget (OMB) requires federal agencies to create and implement a breach notification policy and response plan.¹ This policy establishes OGE's notification policy and response plan for all breaches of PII, regardless of format (e.g., paper, oral, electronic, etc.). It applies to all OGE employees and contractors and all agencies with a Memorandum of Agreement (MOA) for use of an OGE information system, such as *INTEGRITY*.

II. OGE Breach Response Team

Federal agencies are required to establish a breach response team that will convene after a breach occurs. OGE's breach response team consists of its Chief of Staff, Program Counsel², Senior Agency Official for Privacy, Chief Information Officer, Records Officer, and the senior management official of the office responsible for the record(s) in question.

The breach response team is responsible for:

- Determining the extent to which the incident poses problems related to identity theft or loss of individuals' privacy.
- Managing activities to recover from the breach and to mitigate the resulting damage, including decisions relating to external breach notification.
- Determining how incidents involving PII will be tracked within the agency.

III. What is a Breach?

A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.³ Some common examples of a breach include:

¹ See OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017).

² Currently, the Chief of Staff and Program Counsel positions are occupied by the same person.

³ See OMB Memorandum M-17-12.

- A laptop or portable storage device storing PII is lost or stolen
- An email containing PII is inadvertently sent to the wrong person
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits
- An IT system that maintains PII is accessed by a malicious actor
- PII is posted inadvertently on a public website

IV. What is Personally Identifiable Information (PII)?

The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.⁴ It includes, but is not limited to, an individual's date of birth, place of birth, race, religion, weight, employment information, medical information, education information, and financial information.⁵

V. What Should an OGE Employee or Contractor do if a Breach of PII is Suspected or Confirmed?

All OGE employees and contractors are required to **immediately** report any incident that may involve a breach of PII (electronic, oral, or physical) to the Privacy Officer, who will make a risk assessment and determine whether to inform the breach response team. OGE employees are encouraged to fill out the top portion of the attached Incident Reporting Form and provide it to the Privacy Officer.

****Any incident that involves an outside party accessing, modifying, or destroying information in an OGE electronic information system or application must also be concurrently reported to the Chief Information Officer, as well as the Privacy Officer.****

VI. What Should Others who use OGE Information Systems do if a Breach of PII is Suspected or Confirmed?

All agencies using an OGE information system, such as *INTEGRITY*, are responsible for immediately reporting any suspected or confirmed breach of PII to the OGE system manager, as stated in the Memorandum of Agreement between OGE and the agency.

VII. What Happens if Someone Reports a Breach of PII?

Upon the identification of a potential breach of PII, the Privacy Officer shall first determine whether the agency's response can be conducted at the staff level or whether the agency must convene the breach response team. In making this determination, the Privacy Officer will consider the factors discussed in paragraphs C and D, below. These factors include: the nature and sensitivity of the PII, the actors involved and their intent, and the containment

⁴ See OMB Memorandum M-17-12.

⁵ See Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST Special Publication 800-122.

and/or mitigation measures required. If the Privacy Officer determines that referral to the breach response team is not necessary, he or she will document the reasons for that determination on the bottom portion of the Incident Reporting Form. The Senior Agency Official for Privacy will review the Incident Reporting Forms on a periodic basis.

At a minimum, the breach response team must always be convened when a breach constitutes a “major incident.” As defined by OMB, a “major incident” is a breach of PII “that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.”⁶ If the incident involves “any unauthorized modification of any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more people” a determination of “major incident” is required.⁷

Once convened, the Senior Agency Official for Privacy is responsible for leading the breach response team.⁸ The breach response team will take the following actions:

A. Identify the Applicable Privacy Compliance Documentation

The breach response team shall identify any applicable Privacy Act System of Records Notices (SORNs), privacy impact assessments (PIAs), and privacy notices that may apply to the potentially compromised information and any PII that may need to be disclosed as part of the breach response.

B. Report the Breach to the United States Computer Emergency Readiness Team (US-CERT)/National Cybersecurity and Communications Integration Center (NCCIC) and Other Entities as Appropriate

If the breach is determined to be a “major incident,” OGE’s Information Technology Operations Branch shall report it to US-CERT/NCCIC and the OMB Office of the Federal Chief Information Officer (OFCIO) within one hour of determining an incident or breach to be a major incident and should update US-CERT/NCCIC and OMB OFCIO within one hour of determining that an already-reported incident or breach has been determined to be a major incident. US-CERT/NCCIC may be notified by phone, email, or its website.⁹

A notification to US-CERT/NCCIC regarding a physical or electronic breach should include as much of the following information as possible:¹⁰

⁶ See OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements* (October 25, 2018).

⁷ *Id.*

⁸ A copy of this policy and related reference materials are available to the Breach Response Team on the shared drive here: <H:\Breach Response Team Materials>.

⁹ US-CERT can be reached at (888) 282-0870, info@us-cert.gov, and the ‘report an incident’ link on its website.

¹⁰ See United States Computer Emergency Readiness Team, *Federal Incident Reporting Guidelines*, <https://www.us-cert.gov/government-users/reporting-requirements.html> (last viewed October 26, 2018).

- Agency name
- Point of contact information including name, telephone, and email address
- Incident Category Type (e.g., CAT 1, CAT 2, etc.)
- Incident date and time, including time zone
- Source IP, port, and protocol
- Destination IP, port, and protocol
- Operating System, including version, patches, etc.
- System Function (e.g., DNS/web server, workstation, etc.)
- Antivirus software installed, including version, and latest updates
- Location of the system(s) involved in the incident (e.g., Washington DC)
- Method used to identify the incident
- Impact to agency
- Resolution

Depending on the criticality of the incident, it is not always feasible to gather all the information prior to reporting. In that case, the breach response team will continue to report information as it is collected. Reporting should not be delayed to gain additional information.

Major Incidents must also be reported to the appropriate Congressional Committees pursuant Federal Information Security and Modernization Act (FISMA) requirements.¹¹ When appropriate, the breach response team shall also notify and consult with law enforcement.

C. Conduct a Risk Assessment

The breach response team shall assess the likely risk of harm caused by the breach and the level of risk created by the breach. The factors to be considered are described in detail in OMB Memorandum M-17-12. They include the nature and sensitivity of the PII potentially compromised by the breach; the likelihood of access and use of PII, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means; and the type of breach, including the circumstances of the breach, the actors involved, and their intent.

D. Consider How to Best Mitigate the Risk of Harm

Having identified the level of risk, the breach response team shall consider how best to mitigate the identified risks. The breach response team is responsible for advising the Director on an appropriate response plan.

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the agency shall consider what countermeasures it can take, what guidance to provide to affected individuals, and whether there are services the agency can provide. Countermeasures may not always prevent harm to potentially affected individuals but may limit or reduce the risk of harm. For example, if individuals' passwords are potentially compromised in a breach, the agency should require those individuals to change their passwords. With regard to guidance and

¹¹ Detailed guidance on meeting FISMA's Congressional reporting requirements for a breach is provided in OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements* (November 4, 2016).

services, the agency shall consider the guidance options included in Appendix II and III, respectively, of OMB Memorandum M-17-12.

The breach response team shall also consider whether notice to the affected individual(s) is appropriate under the circumstances, balancing the need for transparency with concerns about over-notifying individuals. The agency's decision to offer guidance, take countermeasures, or provide services to individuals potentially affected by a breach may necessarily require the agency to notify those individuals of the breach. However, the agency may also choose to notify individuals even when the agency is not offering guidance or providing a specific service. Weighing all the facts available, notice to affected individuals(s) is warranted when such notice would facilitate appropriate remedial action that is likely to be justified given the risk.

VIII. Notification of Affected Individual(s)

Upon a determination that a breach notification to the affected individual(s) is required, the breach response team shall consider the following five factors:¹²

- Who should provide the notification to the affected individual(s)?
- When should notification be provided?
- What should be included in the notification to the affected individual(s)?
- What means should be used to notify the affected individual(s)?
- Are there any special considerations for the affected population?

A. Who Should Provide the Notification to the Affected Individual(s)?

In general, notification to individuals affected by the breach shall be issued by the OGE Director or a senior-level individual he/she may designate in writing. This demonstrates that the breach has the attention of the head of the agency. Notification involving only a limited number of individuals may also be issued by the Chief Information Officer and/or the Senior Agency Official for Privacy.

When PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor on behalf of an agency is involved in a breach, OGE may require the contractor to notify any potentially affected individuals.

B. When Should Notification Be Provided?

If a determination is made that a notification to the individual(s) affected by a suspected or confirmed breach of PII is warranted, the notification shall be provided as expeditiously as practicable and without unreasonable delay. The breach response team should avoid providing multiple notifications for a single breach and should balance the timeliness of the notification with the need to gather and confirm information about a breach and assess the risk of harm.

C. What Should Be Included in the Notification to the Affected Individual(s)?

¹² See OMB Memorandum M-17-12 for detailed guidance on breach notification.

Every notification must be confirmed in writing and be written in a format that is clear and easy for the recipient to understand. Every notification shall include the following elements:¹³

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of PII compromised by the breach;
- 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;
- 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; and
- Whom potentially affected individuals should contact at the agency for more information, including a telephone number, email address, and postal address.

D. What Means Should Be Used to Notify the Affected Individual(s)?

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. The front of the envelope containing the notification should alert the recipient to the importance of its contents (e.g. “Data Breach Notification Enclosed”).

Telephone: Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

Email: Email notification, especially to or from a non-government email address, is not recommended. However, in limited circumstances it may be appropriate.

Substitute Notification: OGE may provide substitute notification if the agency does not have sufficient contact information to provide notification, or as supplemental notification to keep potentially affected individuals informed. A

¹³ See OMB Memorandum M-17-12 for more information. A Model Breach Reporting Template is included in Appendix I.

substitute notification may consist of a conspicuous posting of the notification on the home page of the agency's website and/or notification to major print and broadcast media. Notification to the 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.

E. Are There Any Special Considerations for the Affected Population?

When a breach potentially affects a vulnerable population, the agency may need to provide a different type of notification to that population, or provide a notification when it would not otherwise be necessary. OGE should give special consideration to providing notice to individuals who are visually or hearing impaired consistent 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.

IX. Consequences for Violating Rules on Safeguarding PII

The failure of OGE employees to fully comply with this policy, and all other agency rules and policies regarding the safeguarding of PII, may result in OGE taking appropriate disciplinary and other measures. An OGE employee may be subject to appropriate disciplinary action if he or she knowingly, willfully, or negligently:

- Fails to implement and maintain security controls for PII, for which he or she is responsible and aware, regardless of whether such action results in the loss of control or unauthorized disclosure of personally identifiable information;
- Exceeds authorized access to PII or discloses it to unauthorized individuals; and/or
- Fails to report any known or suspected loss of control or unauthorized disclosure of PII.

More information regarding OGE employee responsibilities is located in OGE's regulations at 5 CFR §2606.106 OGE employee Privacy Act rules of conduct and responsibilities.

The actions taken in response to an information systems breach should be commensurate with the type of PII involved. The particular facts and circumstances surrounding an incident of breach will be considered in determining an appropriate action. Sanctions may include:

- Removal of Access Authority
- Admonishment;
- Reprimand;
- Suspension;
- Removal; and
- Other actions in accordance with applicable law and agency policy.

Contractors shall be subject to all appropriate and available measures for failure to fully comply with the rules regarding the safeguard of personally identifiable information, which may include removal of the contractor or an individual working for the contractor from OGE's facilities and from the work being performed under the contract.

X. Breach of PII Policy Review and Tabletop Exercises

OGE's breach response team will convene annually, or more often as needed, to review this breach notification policy to ensure that OGE's response to a breach of PII will be effective and to discuss employee training and other mechanisms for preventing incidents of breach. The team will also assess the agency's compliance with its policies on public and internal notifications following a breach of PII and record the results on the attached log.

The Senior Agency Official for Privacy shall annually convene the breach response team to hold a tabletop exercise. 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. Tabletop exercises will 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.

XI. Applicable Law and Guidance

A. The Privacy Act of 1964 (5 U.S.C. § 552a) seeks to uphold and protect the information privacy rights of individuals in regard to records maintained by federal agencies in a system of records that contain personal information.

B. The Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. § 3541 *et seq.*) requires each federal agency to develop, document, and implement an agency-wide program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

C. National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

D. OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

E. OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017.

F. OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018.

G. OMB Memorandum M-16-14, *Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, July 1, 2016.

The Following Officials Have Approved this Document:

1) Shelley Finlayson (Signature) 9/9/19 (Date)

Name: Shelley K. Finlayson
Title: Chief of Staff and Program Counsel

2) Diana Veilleux (Signature) September 6, 2019 (Date)

Name: Diana Veilleux
Title: Senior Agency Official for Privacy and Chief, Legal, External Affairs and Performance Branch and Senior Agency Official for Records Management

3) Ty Cooper (Signature) 2019-09-06 (Date)

Name: Ty Cooper
Title: Chief Information Officer

Review of Compliance with Public and Internal Notification Policies			
Date of Review	Results (In Compliance/Not In Compliance)	SAOP Printed Name	Initials