U.S. OFFICE OF GOVERNMENT ETHICS
BREACH OF PERSONALLY IDENTIFIABLE INFORMATION NOTIFICATION POLICY AND PROCEDURES

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 and contractors to safeguard all personally identifiable information in OGE's possession. Because a breach of personally identifiable information may result in financial loss and personal hardship, it is imperative that OGE protect personally identifiable information in its possession. This policy establishes standardized response and notification procedures which are to be used in the event personally identifiable information is compromised.

Office of Management and Budget (OMB) memorandum M-07-16, dated November 22, 2007, requires federal agencies to create and implement a breach notification policy using a "best judgment" standard. The breach notification policy itemizes procedures for responding to information systems breaches. Federal agencies are required to establish a core response group that will convene after a breach occurs.[1] OMB recommends that this core group include, at minimum, an agency's chief information officer (CIO), chief legal officer, chief privacy officer (or his or her designees), a senior management official from the agency, and the agency's inspector general (or his or her equivalent or designee).[2] In designating a core response group, an agency is assured that it has brought together many of the basic competencies needed to respond to an information systems breach, including expertise in information technology, legal authorities, the Privacy Act, and law enforcement.[3]

II. What is a Breach?

A Breach[4] is 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 an other than authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic.

III. What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including, but not limited to, information about an individual's education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as the individual's name, social security

[1] *See* OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006.
[2] *Id.*
[3] *Id.*
[4] *See* OMB Memorandum M-07-16.

number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.[5]

IV. 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 suspected or confirmed breach of PII, electronic or physical, to the Privacy Officer, Principal Deputy Director, or General Counsel.

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

A. Upon the identification of a potential breach of PII the core response group must meet to evaluate the situation to help guide any further response.[6] OGE's core response group consists of its Principal Deputy Director, General Counsel, Privacy Officer, Chief Information Officer, Records Officer, and the senior management official of the office responsible for the record(s) in question.[7]

B. Every incident involving a suspected or confirmed breach of PII, both in electronic or physical form, must be reported to the United States Computer Emergency Readiness Team (US-CERT) within one hour of its detection or discovery.[8] US-CERT may be notified by phone, email, or its website.[9]

1. A notification to US-CERT regarding a physical or electronic breach should include as much of the following information as possible:[10]

    - Agency name
    - Point of contact information (name, telephone, and email address)
    - Description of the event
    - Incident date and time, including time zone
    - Source IP, port, and protocol
    - Destination IP, port, and protocol
    - Operating System (versions, patches, etc.)
    - System function (e.g. DNS/web server, workstation, etc.)
    - Anti-virus software installed
    - Location of system(s) involved in the incident (e.g. Washington, D.C.)
    - Method used to identify the incident (e.g. IDS, audit log analysis, system administrator)

---

[5] *See* OMB Memorandum M-06-19.
[6] *See* OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006.
[7] OGE does not have an Inspector General.
[8] *See* OMB Memorandum M-06-19. (OMB mandates that no distinction should be made between suspected and confirmed breaches).
[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 February 12, 2013).

- Impact to agency
- Resolution

2. If an incident of breach involves or would potentially pose a threat to another federal agency, a member of the core response group will contact the General Counsel's office in that agency and inform them of the incident.[11]

C. Is Notification to the Affected Person(s) Required?

The core response group will first determine whether sending a breach notification to individuals affected by a suspected or confirmed breach of PII is required by assessing the likely risk of harm caused by the breach and the level of risk created by the breach.[12]

In developing breach notification policies, OMB has directed agencies to apply a "best judgment" standard. OMB does not attempt to set a specific threshold for external notification as breaches are specific and context dependant and notification is not always necessary or desired.[13] For example, OMB draws a distinction between possible loss or compromise of a name and telephone number from a rolodex and the possible loss or compromise of the same information from a medical database. In the first instance, notification to the affected individual would likely not be required. For the second instance, notification would be mandatory.[14]

Based on the OMB guidance, the core response group will evaluate notification considering the following factors:

- The level of ease or difficulty for an unauthorized person to access the PII in light of the manner in which the information was protected[15];
- The means by which the breach occurred, including whether the incident might be the result of criminal activity or likely to result in criminal activity;
- The ability of the Agency to mitigate the identify theft;
- The evidence that the compromised information is actually being used to commit identity theft;
- The potential for harm to the reputation of the affected individual(s); and

[11] See OMB Memorandum M-07-16 (Other public sector agencies may need to be notified, particularly those that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach). For information maintained by the Bureau of Public Debt, the Administrative Resource Center will notify OGE directly of any incidents that have or may have a potential impact on OGE. U.S. Government Interagency Agreement between Office of Government Ethics and the Administrative Resource Center, Bureau of the Public Debt (2012).
[12] *See* OMB Memorandum M-07-16.
[13] *See* OMB Memorandum M-07-16.
[14] *Id.*
[15] Within the context of OGE's mission, the loss of information through compromise of a database or the loss of a non-publicly releasable financial disclosure report or other non-public information collected by OGE in the financial disclosure process would require notification of the affected individual. The inability to locate a publicly releasable financial disclosure report would, however, likely not warrant notifying the filer.

- The potential for harassment or prejudice toward the affected individual(s).[16]

D. When to Notify Affected Person(s)

1. Upon a determination that a breach notification to the affected individual(s) is required, the core response group will address the following five factors before making such an external breach notification to the affected person(s):[17]

    - The timeliness of the notification
    - The source of the notification
    - The contents of the notification
    - The means of providing the notification (e.g. mail, telephone, website, etc.)
    - The recipients of notification: public outreach in response to breach

2. If a determination is made that a notification to the person(s) affected by a suspected or confirmed breach of PII is required, the notification shall be provided without undue delay following the discovery or detection of the suspected or confirmed breach. However, a notification may be delayed if notification could increase the risk of harm to an individual. For example, if the system is still vulnerable to a breach, notification may be delayed to provide time to fix the vulnerability before public notice. A decision to delay notification must be made by the Agency Head or a senior-level individual he or she may designate in writing.[18]

E. Who Provides the Notification to Affected Person(s)?

If notification is required, every individual who is affected by a suspected or confirmed breach of PII must receive actual notice of the incident and of the steps he or she should follow to mitigate any subsequent harm.[19]

1. In general, notification to individuals affected by the breach should be issued by the OGE Director or senior-level individual he/she may designate in writing.[20] This demonstrates the breach has the attention of the chief executive of the organization.[21]

2. Notification involving only a limited number of individuals (e.g., under 50) may also be issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer. This approach signals the agency recognizes both the security and privacy concerns raised by the breach.[22]

---

[16] *See* OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006.
[17] *See* OMB Memorandum M-07-16.
[18] *See* OMB Memorandum M-07-16.
[19] *See* OMB Memorandum M-07-16.
[20] *Id.*
[21] *Id.*
[22] *Id.*

3. When the breach involves a Federal contractor or a public-private partnership operating a system on behalf of OGE, OGE is responsible for ensuring any notification and corrective actions are taken.

F. What is Included in the Notification to the Affected Person(s)?

Every notification shall be confirmed in writing and shall be written in a format that is clear and easy for the recipient to understand.[23] Pursuant to the guidance in OMB Memorandum M-07-16, every notification should include the following elements:

- A brief description of what happened, including the date(s) of the breach and its discovery;
- To the extent possible, a description of the types of PII that were involved in the data breach (e.g. full name, social security number, date of birth, home address, account number, etc.);
- A statement as to whether the information was encrypted or protected by other means when it is determined that such information would be beneficial and would not compromise the security of the records system;
- A brief description of what the Agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
- Who affected individuals should contact at the agency for more information, including a telephone number, e-mail address, and postal address; and
- The steps individuals should take to protect themselves from the risk of identity theft.

G. What Means are used to Notify Affected Person(s)?

Two factors will be considered in determining what sort of notice will be used to notify affected person(s): (1) how many individuals are affected by the breach; and (2) what contact information is available for the affected person(s).[24] In consideration of the guidance provided by OMB, notifications should be provided, based on the circumstances, in the following modes: [25]

1. First-Class Mail

   The use of first-class mail is appropriate when the agency has knowledge of the last known address of the individual who was affected. The front of the envelope containing the notification should alert the recipient to the importance of its contents (e.g. "Data Breach Notification Enclosed"). This should be the primary means of notification.

[23] *See* OMB Memorandum M-07-16.
[24] *See* OMB Memorandum M-07-16.
[25] *Id.*

2. E-mail

   If an individual has provided the agency with an e-mail address and requested that correspondence be sent in this manner, notifications can be sent using this medium. While notification by e-mail is discouraged, it may be necessary to send notifications when time is of the essence or when other media are not appropriate or available.

3. Substitute Notice

   Providing notification of a breach through a public announcement, website or distribution to public service, or other membership organizations can be useful when the agency does not have sufficient contact information for the affected individual to make a notification by mail or e-mail. Substitute notice should consist of a conspicuous posting of the notice on the home page of the agency's website and notification to major print and broadcast media. The notice to the media should include a toll-free number where an individual can learn whether or not his or her information is included in a breach.

4. 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. OGE policy encourages the use of notification by telephone where possible. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

5. Reasonable Accommodations under Rehabilitation Act of 1973

   In order to provide notice to individuals' who are hearing or visually impaired, OGE will take the necessary steps to ensure that all individuals affected by a breach of PII receive notification. OGE will use the guidance provided for in OMB Memorandum *Recommendations for Identity Theft Related Data Breach Notification* to ensure the agency's actions are appropriately tailored to the particular circumstances.[26]

H. Who Receives Notification?

1. Pursuant to a determination that notification is required, every individual who is affected by a suspected or confirmed breach of PII must receive actual notice of the incident and of the steps he or she should follow to mitigate any subsequent harm.[27]

2. If it is determined that the public should be informed about an incident of breach, the agency should post information about the breach, notification process, and steps taken to remedy the issue on the OGE website in a timely fashion. The

[26] OMB suggests that possible accommodations can include establishing a Telecommunications Device (TDD) for the hearing impaired or positing notifications in large type for the visually impaired.
[27] *See* OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006.

posting should, as appropriate, include a link to Frequently Asked Questions and other talking points to assist the public's understanding of the breach and notification processes. The information should also appear on the www.USA.gov website.[28]

VI. Reducing the Risk of Harm after a Breach

Depending on the circumstances, a broad range of harms can result after a breach. Due to the fact that the effects of a breach can persist, it is imperative action is taken to ensure that any harm experienced by an affected individual is minimal.

A. Individual Actions

Individuals affected by a breach have numerous options available to them that can be taken in order to minimize any harm. In notifying an affected individual, OGE should recommend options, in accordance with guidance set forth in OMB Memorandum *Recommendations for Identity Theft Related Data Breach Notification*, that an individual can pursue to minimize any damage to their person or property, including:

- Contact financial institution(s) to determine whether account(s) should be closed.
- Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.
- Request a free credit report at www.AnnualCreditReport.com or by calling1-877-322-8228. Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus (Equifax, Experian, and TransUnion) for a total of three reports every year. The annual report can be used as a self monitoring tool as well as a way to check credit without initiating a fraud alert.
- Place a fraud alert on the credit reports maintained by the three major credit bureaus. This option is most useful when the breach includes information that can be used to open new accounts, such as social security numbers. The alert signals credit issuers who obtain credit reports that they should take steps to verify the consumer's identity before issuing credit.
- Place a credit freeze on their credit file. Doing so precludes third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.
- Review resources provided on the Federal Trade Commission (FTC) identity theft website at www.ftc.gov/idtheft .
- Be aware that the public announcement of the breach could itself cause criminals, under the guise of providing legitimate assistance, to use various

[28] *See* OMB Memorandum M-07-16.

techniques, including the telephone and email, to deceive the individuals affected by the breach into disclosing their credit card numbers, bank account information, social security numbers, or other personal information. One common such technique is "phishing," a scam involving an email that appears to come from a bank or other organization that asks the individual to verify account information, and then directs the individual to a fake website whose only purpose is to trick the individual into divulging his/her personal information. *See* FTC's web site at http://www.ftc.gov/bep/edu/pubs/consumer/alerts/alt166.htm for information on this type of fraud.

B. Agency Actions

OGE will to take the following steps to ensure that any harm resulting from a breach is mitigated:

- If the breach involves government-authorized credit cards, the agency will notify the issuing bank promptly; and
- If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, the agency will notify the bank or other entity that handles that particular transaction for the agency.[29]

VII. Safeguarding PII (Rules and Consequences)

The failure of OGE employees to fully comply with the rules regarding the safeguard of personally identifiable information will result in OGE taking all appropriate and available disciplinary and other measures.

A. If appropriate, an OGE employee shall be subject to appropriate disciplinary action if he or she knowingly, willfully, or negligently:

- Fails to implement and maintain security controls, for which he or she is responsible and aware, for PII regardless of whether such action results in the loss of control or unauthorized disclosure of personally identifiable information;
- Exceeds authorized access to, or discloses to unauthorized persons, PII;
- Fails to report any known or suspected loss of control or unauthorized disclosure of PII; and/or
- For managers, fails to adequately instruct, train, or supervise employees in

[29] *See* OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006 (It is recommended that agencies institute mechanisms to minimize harm to an individual after a breach including data breach analysis technology and credit monitoring services).

their responsibilities.[30]

B. 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.

C. Consequences of 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. At a minimum, access authority should be removed from any individual demonstrating reckless disregard or a pattern of error in safeguarding PII.[31] However, other sanctions may include:

- Admonishment;
- Reprimand;
- Suspension;
- Removal; and
- Other actions in accordance with applicable law and agency policy.[32]

VIII. Breach of PII Policy Review

OGE's core response group will convene quarterly, 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.

IX. 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. The Act requires each federal agency to: (1) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records; (2) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to the records' security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; and (3) maintain system of records that encompass personally identifiable information in a manner that is accurate, relevant, timely, and complete, including through the use of notices to the public.

[30] *See* OMB Memorandum M-07-16.
[31] *See* OMB Memorandum M-07-16.
[32] *Id.*

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.[33] Specifically, in response to incidents involving personally identifiable information, FISMA requires each federal agency to: (1) implement procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done;[34] (2) notify and consult with the Federal information security incident center, law enforcement agencies and Inspectors General, an office designated by the President for any incident involving a national security system and any other agency or office in accordance with the law or as directed by the President;[35] and (3) implement National Institute of Standards and Technology guidance and standards.[36]

[33] *See* National Institute of Standards and Technology, *FISMA Detailed Overview*, http://csrc.nist.gov/groups/SMA/fisma/overview.html (last updated May, 16 2012).
[34] *See* 44 U.S.C. § 3544(a)(1)-(2).
[35] *See Id.* § 3544(b)(7).
[36] See *Id.* § 3544 (b)(2)(D)(ii).