



ADMINISTRATIVE COMMUNICATIONS SYSTEM  
U.S. DEPARTMENT OF EDUCATION

**DEPARTMENTAL DIRECTIVE**

OM:6-107

Page 1 of 46 (04/15/2008)

*Distribution:*  
All Department of Education Employees

*Approved by:*           /s/ by Chris Marston            
Michell Clark  
Assistant Secretary for Management

**External Breach Notification Policy and Plan**

*Table of Contents*

I.	Purpose.....	2
II.	Policy .....	2
III.	Authorization .....	3
IV.	Applicability .....	3
V.	Definitions.....	3
VI.	Responsibilities.....	5
VII.	Procedures and Requirements.....	8
	Appendix A – OMB M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information .....	19
	Appendix B - OMB M-07-04 ("Use of Credit Monitoring Services Blanket Purchase Agreements (BPA)" .....	41
	Appendix C: Federal Trade Commission Links .....	46

## I. Purpose

This Directive establishes an external breach notification policy and plan for the United States Department of Education (ED). Based on this Directive, ED shall promptly and effectively determine whether or not to notify affected parties outside ED of a suspected or actual breach of personally identifiable information (PII)<sup>1</sup> that ED maintains or processes. This policy applies to all PII maintained, collected, used, or disseminated by ED in any format. This plan also details the related procedures by which affected parties will be notified should such an event occur.

When a data breach involving PII occurs, ED will conduct a risk analysis. Based on this risk analysis ED will determine whether to notify individuals whose PII may have been involved in the breach and what steps if any ED will take to mitigate actual or potential harm.

The procedures in this directive supplement the procedures already stated in:

Handbook for Information Security Incident Response and Reporting Procedures  
[http://connected.ed.gov/document\\_handler.cfm?id=3775](http://connected.ed.gov/document_handler.cfm?id=3775),

Handbook for Information Assurance Security Policy  
[http://connected.ed.gov/document\\_handler.cfm?id=3569](http://connected.ed.gov/document_handler.cfm?id=3569)

Handbook for Protection of Unclassified Sensitive Information  
[http://connected.ed.gov/document\\_handler.cfm?id=6366](http://connected.ed.gov/document_handler.cfm?id=6366)

## II. Policy

It is the policy of ED that:

- A. ED shall assess all actual or suspected data breaches involving PII that is processed or maintained by ED, and shall make a determination as to whether external notification, or any other remediation, is required.
- B. The determination of whether external notification is required shall be based on a risk assessment performed by ED's Privacy Incident Response Team (PIRT), or in some circumstances, the Secretary.
- C. A risk analysis shall consider, among other things, the likelihood that the information will be used to harm the subject of the data.

---

<sup>1</sup> **Personally Identifiable Information**, in accordance with the definition prescribed by OMB M-07-16, cited above, is any information about an individual, processed or maintained, which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Refer to [OCIO's Handbook for Information Security Incident Response and Reporting Procedures](#), OCIO-14, for discussion of security measures for the protection of privacy data.

- D. The PIRT shall apply the five risk factors described in Section VII, 3.e , within the fact-specific context of a reported actual or suspected breach of PII. Using this methodology, notification shall be given in instances where there is reasonable risk of harm.
- E. If the PIRT determines that the incident meets the established criteria for notification, and, thus, recommends that external notification is appropriate, such notification shall be done as soon as practicable after the data breach.

### III. Authorization

- A. Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007. <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>
- B. Memorandum [not numbered] "Recommendations for Identity Theft Related Data Breach Notification," September 20, 2006. [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf)
- C. Title III of the E-Government Act of 2002, Pub. L. 107-347, "Federal Information Security Management Act of 2002" (FISMA). [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ347.107](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107)
- D. Privacy Act of 1974, as amended (5 U.S.C. § 552a). <http://www.usdoj.gov/oip/privstat.htm>

### IV. Applicability

This directive applies to all ED employees, and all contractors who process or maintain PII on behalf of ED.

### V. Definitions

- A. **Accelerated Notification** is the exception process through which the Secretary determines that there has been a significant, intentional breach, or that there is an immediate, substantial risk of identity theft or other significant harm, of the individual(s) whose data was the subject of the data breach. If the Secretary determines that such a breach has occurred, the Secretary can accelerate the notification and the performing of other mitigations, such as credit monitoring and deletion of data.
- B. **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

- C. **Data breach** is an incident considered to have occurred when there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any other similar act where persons (other than authorized users and for other than the authorized purpose), have access, or potential access, to PII, whether in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.
- D. **Data breach analysis** means the process used to determine the extent and impact of a data breach resulting from an actual or suspected breach of personally identifiable information.
- E. **ED** means the United States Department of Education.
- F. **External Notification** is the notice provided to those individuals outside of ED after a data breach involving PII has occurred, and a risk assessment indicates that such notice is appropriate. External notification includes notice to affected data subjects, and may also include notification to the general public through the news media, ED's webpage or notice to Members of Congress. External notification, in this case, does not include notification of the Inspector General and law enforcement, as they will have already been notified pursuant to the *Handbook for Information Security Incident Response and Reporting Procedures*. Handbook OCIO-14 [http://connected.ed.gov/document\\_handler.cfm?id=3775](http://connected.ed.gov/document_handler.cfm?id=3775).
- G. **Identity theft** means a fraud committed using the identifying information of another person, subject to such further definition as the Federal Trade Commission may prescribe, by regulation.
- H. **Information system**, as defined by OMB Circular A-130, means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.
- I. **Integrity** means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- J. **Processed or maintained by ED** means created, received, stored, transmitted, or manipulated by ED personnel or by a person acting on behalf of ED, including a contractor or other organization or any level of subcontractor or other sub-organization.
- K. **Secretary** means the Secretary of Education, or as designated by the Secretary, either the Deputy Secretary or the Under Secretary.
- L. **Suspected Breach** means a data breach, as defined in 5. C. above, that may have occurred.

- M. **Unauthorized access** is when a person gains logical or physical access without permission to PII, or to a network, system, applications, data, or other resource containing PII. Logical access means being able to interact with data through access control procedures such as identification, authentication, and authorization. Physical access means being able to physically touch and interact with the computers and network devices.

## VI. Responsibilities

### A. Secretary

The Secretary shall make final decisions regarding breach notification and any remediation of incidents where the PIRT determines that the risk of harm is high, or the incident is widespread, or both. The Secretary shall also determine whether to use accelerated notice.

### B. EDCIRC Coordinator

ED's Computer Incident Response Capability (EDCIRC) Coordinator, working within the Office of the Chief Information Officer (OCIO), Information Assurance, coordinates ED's response to all information security incidents. Upon learning of an information security breach that involves PII, or is suspected to have involved PII, the EDCIRC Coordinator, pursuant to the OCIO directive, is responsible for notifying the Office of Inspector General and the Privacy Advocate, of the breach. The EDCIRC Coordinator shall provide to the PIRT any relevant incident information collected during the investigation of the security incident for the team's risk analysis and shall determine if there is sufficient information to be able to make the external notification determination.

### C. Senior Agency Official for Privacy

The Senior Agency Official for Privacy (SAOP) is the Assistant Secretary for Management. The SAOP is responsible for convening and chairing meetings of the PIRT, reporting the PIRT's findings and recommendations to the Secretary, reviewing the status of all notifications, and jointly, with the Chief Information Officer (CIO), issuing notifications of those incidents that the risk of harm are low or moderate, and/or are not widespread. The SAOP is accountable to the Secretary for the appropriate handling of any breach incident, and for the continuing review and improvement of the breach notification policy.

### D. Privacy Incident Response Team (PIRT)

The PIRT is chaired by the Senior Agency Official for Privacy. The team consists of the CIO, ED's Privacy Advocate, the Senior Official of the program experiencing the breach, the Assistant Secretary for Communications and Outreach, the Assistant Secretary for Legislation and Congressional Affairs, and, as needed, the General

Counsel, the Inspector General, the Deputy Assistant Secretary for Management, and the Chief Financial Officer, or their designees. The PIRT shall do the following:

1. In the event of an actual or suspected loss of PII, the Chair shall convene the PIRT to conduct a risk analysis using the OMB criteria, as detailed in this Directive, to determine the likelihood the incident might result in identity theft, consumer fraud, or other harm.
2. The PIRT is divided into two groups - core members and ancillary members. The core members serve as the permanent team for all PIRT purposes including annual meetings to review this Directive, as well as meetings convened to address a breach. Ancillary members are officials from other key Principal Organizations who serve on an as needed basis to provide essential expertise. Core members are: the SAOP, the CIO, the Privacy Advocate, the Senior Official of the program experiencing the breach, the Assistant Secretary of Communications and Outreach, and the Assistant Secretary of the Office of Legislation and Congressional Affairs. The Ancillary members are the General Counsel, the Inspector General, the Deputy Assistant Secretary for Management, the Chief Financial Officer, and senior officials from FSA and IES.
3. The PIRT shall review the information provided by the EDCIRC Coordinator, conduct the required risk analysis, and document its findings.
4. Based on its findings, the PIRT shall determine whether it is appropriate to issue external notification, or to recommend to the Secretary to do so, as circumstances require.
5. Each PIRT member, both core and ancillary, shall designate an alternate(s) to serve as a representative when the member is unable to participate in PIRT activities. It is the responsibility of each PIRT member to ensure that he or she is represented at each PIRT meeting.
6. Any report or official communication from the PIRT shall be signed by the SAOP or designee.
7. The PIRT shall meet annually to review this directive, any changes in circumstances that would require amendment of this directive, the handling of any breaches that occurred during the year, incident trends, and proposed process improvements.

**E. Chief Information Officer**

The CIO, or designee, shall participate in all PIRT activities, and shall, with the SAOP, issue external notifications for incidents that are of low or moderate impact, and/or are not widespread.

**F. ED's Privacy Advocate**

The Privacy Advocate, or designee, working within the Office of Management, Regulatory Information Management Services, will be notified by the EDCIRC Coordinator that a suspected or actual breach involving PII has occurred, and shall consult with the EDCIRC coordinator to monitor initial fact finding. The Privacy Advocate provides insight and guidance regarding breach risk analysis, external notification, and provides information on current issues, trends, best practices and requirements regarding privacy safeguards. The Privacy Advocate shall also participate in all PIRT activities, and will maintain a record of PIRT actions. The Privacy Advocate is responsible to the SAOP for appropriate coordination of PIRT activities and for the continuing review and improvement of the breach notification policy.

**G. Senior Official of the Program Experiencing the Breach**

The Senior Official of the Program experiencing the Breach, or designee, shall provide any program information needed, and shall participate in the PIRT review and decision-making process. If it is determined that ED will provide external notification, the Official shall be responsible for developing the external notification letter, developing the list of the names and addresses of those being notified, and overseeing dispatch of the notice to the individual(s) involved. This official or designee shall be authorized to represent the interests of the principal organization for the purposes of decision-making regarding mitigation activities and funding issues.

**H. Assistant Secretary for Communications and Outreach**

The Assistant Secretary, or designee, shall participate in all PIRT activities. The Assistant Secretary shall also recommend a public notification strategy, as needed, and shall develop outreach materials, e.g., news releases, webpage postings.

**I. Assistant Secretary for Legislation and Congressional Affairs**

The Assistant Secretary, or designee, shall participate in all PIRT activities. The Assistant Secretary shall also provide assistance with communicating with Congress, and in responding to Congressional inquiries.

**J. General Counsel (GC)**

The General Counsel, or designee, shall participate in PIRT activities, in order to provide legal counsel regarding external notification.

**K. Inspector General (IG)**

The Office of Inspector General is the law enforcement component of ED and has primary responsibility for criminal investigations related to ED's programs and

operations. As such the IG, or designee, shall participate in PIRT activities, coordinate any law enforcement response and provide input regarding external notification.

**L. Deputy Assistant Secretary for Management**

The Deputy Assistant Secretary, or designee, shall participate in PIRT activities, in order to provide expertise on Office of Management matters, and shall provide input regarding external notification.

**M. Chief Financial Officer (CFO)**

The CFO, or designee, shall participate in PIRT activities and shall provide input regarding external notification and contract issues.

**N. FSA and IES Officials**

FSA and IES Officials shall participate at annual meetings and other PIRT discussions as necessary, in order to provide expertise from their roles as the major collectors and users of data within ED.

## **VII. Procedures and Requirements**

Upon notice that a breach involving PII, or suspected to involve PII, has been reported, the PIRT must determine the course of action regarding external notification. The procedures required of the PIRT can be found in the procedures and flowchart immediately following the procedures.

**A. Internal Notification**

1. Information security breaches, including those involving PII, are required to be reported to the OCIO<sup>2</sup>.
2. When a breach, or suspected breach, involving PII has been reported to the EDCIRC Coordinator, the Coordinator provides initial and follow-up facts to the Privacy Advocate describing the incident.
3. The Privacy Advocate shall notify the PIRT Chair and shall consult with the Chair about the most recent incident findings.

**B. Convening the PIRT** - The Chair shall convene a meeting of the PIRT as soon as reasonably possible, but no later than two working days after the Chair determines

---

<sup>2</sup> All information security breaches or incidents are immediately reported to the EDCIRC Coordinator, in accordance with *the Handbook for Information Security Incident Response and Reporting Procedures*. Handbook OCIO-14, or replacement publication. The EDCIRC Coordinator reports the incident as required, including to the Incident Handler, who will conduct a review of the incident. A security risk assessment is performed.



that there is sufficient information to conduct the required analysis. For the purposes of conducting PIRT meetings, the Chair may convene via conference call, email, or on-site in order to accommodate the schedules of the members and the urgency of the agenda item(s).

**C. The PIRT determines whether external notification is appropriate.**

1. **Intentional loss and determination that data were the target** – If the PIRT is informed that the breach was intentional, and data were the target, the SAOP, after concurrence from the OIG, shall recommend to the Secretary that the accelerated process be performed (see Accelerated Process, Section VII. J.). Any notification actions shall have the concurrence of the General Counsel, the Inspector General, law enforcement, and any others as required.
2. **Under all other circumstances** the PIRT shall proceed with the risk analysis as described below.
3. **Risk Analysis**
  - a. The PIRT shall first assess the likely risk of harm caused by the breach, using the five factors described below, and then assess the level of risk – as low, moderate, or high.
  - b. In determining the risk of harm, the PIRT shall consider a wide variety of harms, including harm to reputation and the potential for harassment or prejudice, particularly when health or financial information is involved in the breach.
  - c. If there is little or no risk of harm, or when notification could increase a risk of harm, notification shall be delayed while appropriate safeguards are put in place.
  - d. The five factors, described in detail below, that the PIRT shall consider assessing the likely risk of harm are:
    - i. Nature of the Data Elements Breached
    - ii. Number of Individuals Affected
    - iii. Likelihood the Information is Accessible and Usable
    - iv. Likelihood the Breach May Lead to Harm
    - v. Ability of the Agency to Mitigate the Risk of Harm
  - e. The PIRT shall consider the following five factors to assess the likely risk of

harm:

- i. **Nature of the Data Elements Breached.** The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. In assessing the levels of risk and harm, the PIRT shall consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.
- ii. **Number of Individuals Affected.** The magnitude of the number of affected individuals may dictate the method that is chosen for providing notification, but should not be the determining factor for whether ED provides notification.
- iii. **Likelihood the Information is Accessible and Usable.** The PIRT shall assess the likelihood that PII will be, or has been, used by unauthorized individuals. An increased risk that unauthorized individuals will use the information should influence ED's decision to provide notification. The PIRT shall consider any physical, technological, and procedural safeguards that were in place, such as properly implemented encryption. In considering if the safeguards provided protection that makes the PII inaccessible or unusable, the PIRT must assess whether the PII is at a low, moderate, or high risk of being compromised. The assessment shall be guided by the Director of Information Assurance Services, and shall comply with National Institute of Standards and Technology (NIST) security standards and guidance. Other considerations may include the likelihood that any unauthorized individual will know the value of the information and will either use the information or sell it to others.
- iv. **Likelihood the Breach May Lead to Harm**
  - (a) ***Broad Reach of Potential Harm.*** The PIRT shall consider whether the breach could result in substantial harm, embarrassment, inconvenience, or unfairness to any of the subject individuals. The PIRT shall also consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information that could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.
  - (b) ***Likelihood Harm Will Occur.*** The likelihood that a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security

numbers and account information are useful for committing identity theft, as are dates of birth, passwords, and mother's maiden names. If the information involved is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of patients at a clinic for treatment of a contagious disease. In considering whether the loss of information could result in identity theft or fraud, the PIRT should consult guidance from the Identity Theft Task Force.<sup>3</sup>

- v. **Ability of the Agency to Mitigate the Risk of Harm.** Within an information system, the risk of harm will depend on how ED is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and difficult to determine.

#### 4. **Reassess the Level of Impact Assigned to the Information.**

- a. After evaluating each of these factors, the PIRT shall review and reassess the level of impact that has already been assigned to the information using the impact levels for system security, (as opposed to breach impacts), defined by NIST. The impact levels – low, moderate, and high, -- describe the potential impact(s) on an organization or individual if a breach of security occurs.
  - i. **Low:** the loss of confidentiality, integrity, or availability is expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
  - ii. **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
  - iii. **High:** the loss of confidentiality, integrity, or availability is expected to have a **severe** or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- b. The impact levels will help determine when and how notification shall be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification shall give greater weight to the likelihood that the information is accessible and usable and whether the breach may lead to

---

<sup>3</sup> Memorandum [not numbered] "Recommendations for Identity Theft Related Data Breach Notification," September 20, 2006 [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf)

harm.

- c. Once the determination has been made about whether or not external notification will be provided, the PIRT Chair is responsible for making sure that they appropriate parties are notified and the notification is made according to the PIRT's determination.
- d. The PIRT shall apply the five risk factors within the fact-specific context of a reported actual or suspected breach of PII. Using this methodology, it is ED policy that notification shall be provided in instances where there is reasonable risk of harm.

**D. Mitigation and Related Actions** – The PIRT's analysis should also include consideration of appropriate mitigation options. Such options may include:

1. **External Notification** – This process is described in detail below.
2. **Credit Monitoring** – If it is determined that credit monitoring services are appropriate, the Program Office experiencing the breach shall, if needed, utilize one of the government-wide Blanket Purchase Agreements that GSA has established to provide these services.<sup>4</sup>
3. **Law Enforcement Notification -Law Enforcement Notification** - The Office of Inspector General, as the primary law enforcement component of ED, shall determine the appropriate steps, if needed, for coordination with any other law enforcement agencies.
4. **Other Mitigation** - ED may also set up a toll-free number to handle inquiries from the affected individuals and the public, may remove subject PII if no longer needed for documented agency need, etc.

**E. Timeliness of the Notification** - The catalyst for ED's response to a breach involving PII, is the OCIO's requirement for reporting information security incidents immediately upon discovery. This policy can be found in Handbook OCIO-14 Information Security, Incident Handling Procedures that specifies that actual or suspected information breaches must be reported within one hour. Upon notification that a breach involving PII has occurred or is suspected to have occurred, and a risk analysis supports external notification, ED shall provide notification without unreasonable delay. Such notification shall be consistent with the needs of law enforcement and national security, and any measures necessary to restore the reasonable integrity of any computerized data system compromised. Decisions to delay notification shall be made by the Secretary or by a senior-level individual designated in writing by the Secretary. In some circumstances, law enforcement or national security considerations may require a delay if notification would seriously impede the investigation of the breach or the affected individual(s). However, any

---

<sup>4</sup> See Appendix D, OMB M-07-04, December 22, 2006.

delay shall not exacerbate risk or harm to any affected individual(s).

F. **Source of the Notification** - If the impact on affected individuals is high, or the breach is widespread, notification to individuals affected by the breach shall be issued by the Secretary or designee. If the notification involves a limited number of individuals, or the impact is low or moderate, notification may also be issued jointly under the auspices of the SAOP and the CIO.

G. **Contents of the Notification** - The notification shall be provided in writing, with few exceptions, as described in the next section – “Means of Providing Notification”, and shall be concise, conspicuous, and in plain language. Two sample notification letters appended below that can be used as models. The PIRT shall determine whether to include additional details in a Frequently Asked Question (FAQ) format, or through ED’s website. If it is known that the affected individual(s) are not English proficient, notice shall also be provided in the appropriate language(s). The notice shall include the following elements:

1. A brief description of what happened, including the date(s) of the breach and of its discovery;
2. To the extent possible, a description of the types of personal information involved in the breach (*e.g.*, full name, Social Security number, date of birth, home address, account number, or disability code.);
3. A statement clarifying whether the information was encrypted or protected by other means and on when it is determined that such information would be beneficial and would not compromise the security of the system;
4. What steps individuals should take to protect themselves from potential harm, if any. Such steps may include referring them to the FTC’s identity theft webpage. <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html>;
5. What ED is doing, if anything, to investigate the breach, mitigate losses, and protect against any further breaches; and
6. The points of contact at ED for more information, which may include a toll-free telephone number, e-mail address, or postal address.

#### H. Means of Providing Notification

##### 1. First-class mail

- a. Notification to the last known mailing address of the individual(s) in ED’s records is the primary means of external notification.
- b. If there is reason to believe the address is no longer current, ED shall take

reasonable steps to update the address by consulting with other agencies such as the US Postal Service.

- c. The notice shall be sent separately from any other mailing so that it is conspicuous to the recipient.
- d. If ED is using another agency to facilitate mailing (for example, consulting the Internal Revenue Service for current mailing addresses of affected individuals), ED, and not the facilitating agency, must be identified as the sender.
- e. The front of the envelope shall be labeled to alert the recipient to the importance of its contents, *e.g.*, “Data Breach Information Enclosed” and shall be marked with the U.S. Department of Education as the sender in order to reduce the likelihood that the recipient thinks it is advertising mail.

## 2. Telephone

In cases where the impact is not widespread, but where the harm may be great, and the issue is urgent, the telephone may be the most appropriate means of notification. In these cases, written notification by first-class mail shall follow as soon as practicable.

## 3. Email

- a. The notification shall not be provided by e-mail, unless an individual has provided an e-mail address, and expressly has consented to use e-mail as the primary means of communication with ED, and no known mailing address is available.
- b. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. For example, if the matter is urgent, the risk of harm is great, and there are large numbers of people affected the Department might use both regular mail and e-mail to reach an individual.
- c. If a decision is made to use e-mail, such notification may include links to ED’s website and <http://www.usa.gov> web sites, where the notice may be “layered” so that the most important summary facts are up front with additional information provided under link headings.

## 4. Existing Government-Wide Services

In addition to the means discussed above, ED should use Government-wide services already in place to provide support services needed, such as USA Services, including the toll free number 1-800-FedInfo and <http://www.usa.gov>.

## 5. Newspapers or other Public Media Outlets

The PIRT shall determine whether supplementing individual notification, such as with notification in newspapers or other public media outlets, is appropriate.

## 6. Substitute Notice

If ED does not have sufficient contact information to provide individual notification, substitute notice may be used. Substitute notice shall consist of a conspicuous posting of the notice on the <http://www.ed.gov> home page and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media may include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

## 7. Accommodations

Special consideration must be given to providing notice to individuals who are visually or hearing impaired consistent with section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a telephone number for those who use a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on ED's website.

# I. Who Receives Notification: Public Outreach in Response to a Breach

1. **Notification of Individuals.** The PIRT shall determine to whom notice shall be provided. Parties may include the affected individuals, the public media, and/or other third parties (such as Members of Congress, academic institutions, financial partners, etc.) affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals must be notified promptly.
2. **Notification of Third Parties including the Media.** If it is determined that a third party will be notified regarding a breach, the PIRT shall consider the following:
  - a. **Careful Planning.** ED's decision whether or not to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. The Office of Communications and Outreach shall ensure prompt disclosure to the media wherever a decision is made to provide such third-party notification. When appropriate, public media shall be notified as soon as possible after the discovery of a breach and after the response plan, including the notification, has been developed. The Office of Communications and Outreach shall develop the notification and focus on

providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above.

- b. **Web Posting.** The Office of Communications and Outreach shall develop and post information about the breach and notification in a clearly identifiable location on ED's home page, as appropriate, as soon as possible after a decision is made to provide notification to the affected individuals. The posting shall also include a link to Frequently Asked Questions (FAQs) and other information to assist the public's understanding of the breach and the notification process. The PIRT shall also consider posting the information to the www.USA.gov web site. The PIRT shall also consult with GSA's USA Services regarding using that agency's call center.
- c. **Notification of other Public and Private Sector Agencies.** The PIRT may determine that other public and private sector agencies should be notified on a need-to-know basis, particularly those agencies that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach.
- d. **Congressional Inquiries.** The Office of Legislation and Congressional Affairs shall take the lead in developing responses to potential inquiries from Members of Congress

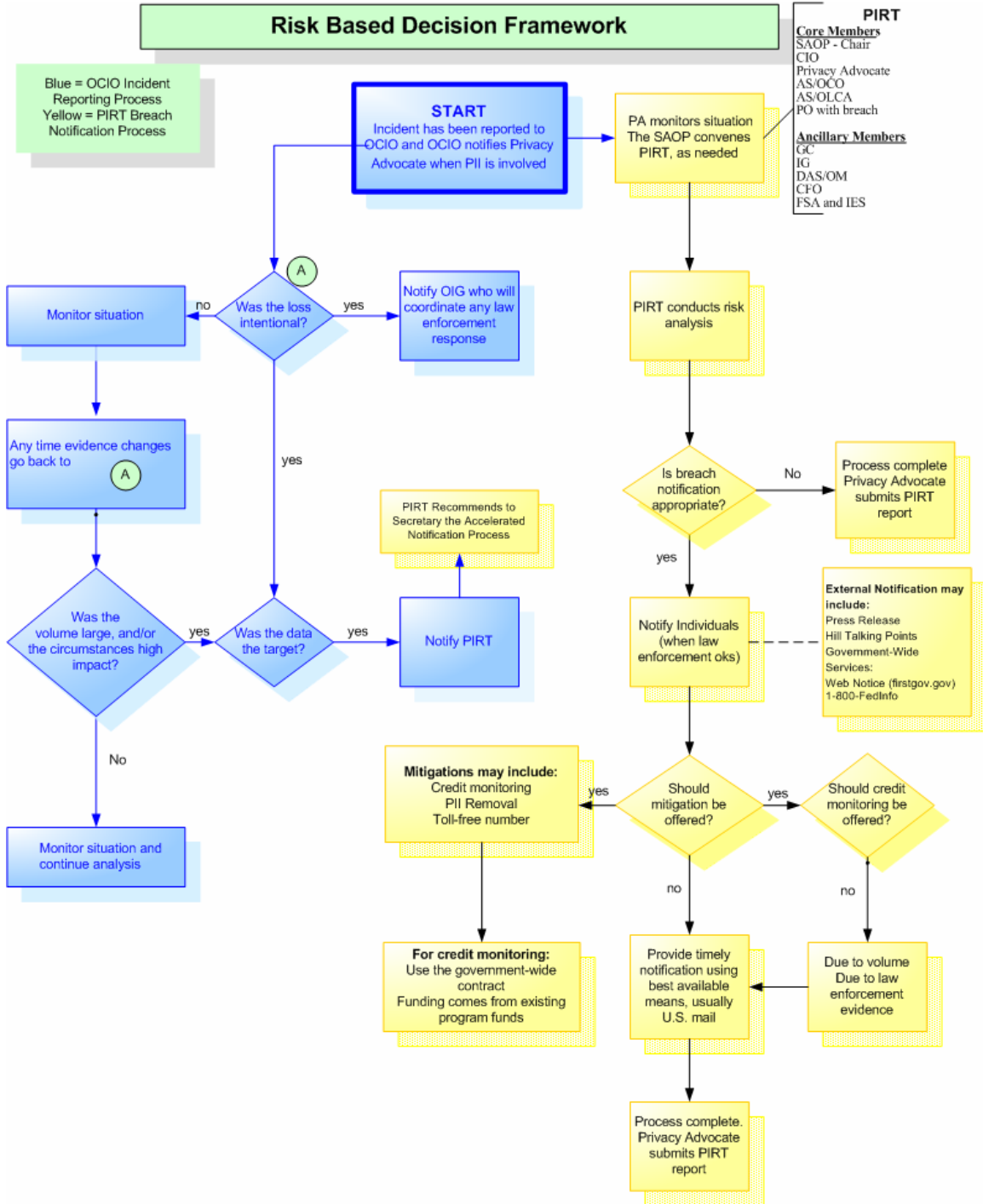
#### J. Accelerated Notification

1. If it is determined that the breach was intentional and the data were the target, or if after the risk assessment has been completed, it is apparent that the risk of significant harm is high or is widespread, the PIRT Chair shall promptly inform the Secretary.
2. If the Secretary, or delegated authority, based on the information available to ED, agrees that there has been a significant intentional breach, or that there is an immediate, substantial risk of identity theft or other significant harm, to the individuals whose data were the subject of the data breach, the accelerated notification will be performed.
3. If the Secretary determines that providing timely notice may enable the record subjects to promptly take steps to protect themselves, or that the offer of credit protection services will assist in timely mitigation of possible harm to individuals from the data breach, the Secretary may provide such notice and or offer them credit protection services, on a case-by-case basis, prior to the performance of the risk analysis described above.
4. In determining whether to promptly notify individuals and to offer them credit protection services, the Secretary shall make the decision based upon the totality



of the circumstances and information available to the Secretary at the time of the decision, including information on whether providing notice and offering credit protection services would be likely to assist record subjects in preventing or mitigating the results of identity theft based on the compromised PII. The Secretary's exercise of this discretion will be based on good cause, including consideration of some of the following factors:

- a. The nature and content of the lost, stolen, or improperly accessed data, e.g., the data elements involved, such as name, social security number, and date of birth;
- b. The ability of an unauthorized party to use the lost, stolen, or improperly accessed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects.
- c. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- d. Ease of physical access to the lost, stolen, or improperly accessed data, e.g., the degree to which the data are vulnerable to unauthorized access, such as being discarded in a public dumpster, or left unattended at a copying or FAX machine;
- e. The format of the lost, stolen, or improperly accessed data, e.g., in a standard electronic format, such as ASCII, or on paper;
- f. Evidence indicating that the lost, stolen, or improperly accessed data may be the target of unlawful acquisition; and/or
- g. Evidence that the same or similar data was acquired from other sources improperly and used for identity theft.



## Appendix A – OMB M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D. C. 20503

DEPUTY DIRECTOR  
FOR MANAGEMENT

May 22, 2007

M-07-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III  
Deputy Director for Management

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Safeguarding personally identifiable information<sup>1</sup> in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA)<sup>2</sup> and the Privacy Act of 1974.<sup>3</sup>

As part of the work of the Identity Theft Task Force,<sup>4</sup> this memorandum requires agencies to develop and implement a breach<sup>5</sup> notification policy<sup>6</sup> **within 120 days**. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy<sup>7</sup> while ensuring proper safeguards are in place to protect the information. Agencies should

<sup>1</sup> The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

<sup>2</sup> Title III of the E-Government Act of 2002, Pub. L. No. 107-347.

<sup>3</sup> 5 U.S.C. § 552a.

<sup>4</sup> Executive Order 13402 charged the Identity Theft Task Force with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions which can be taken by the public and private sectors. On April 23, 2007 the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at [www.idtheft.gov](http://www.idtheft.gov).

<sup>5</sup> For the purposes of this policy, the term "breach" is used to include 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.

<sup>6</sup> Agencies should use a best judgment standard to develop and implement a breach notification policy. Using a best judgment standard, the sensitivity of certain terms, such as personally identifiable information, can be determined in context. For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. Similarly, using a best judgment standard, discarding a document with the author's name on the front (and no other personally identifiable information) into an office trash can likely would not warrant notification to US-CERT.

<sup>7</sup> Terms not specifically defined within this Memorandum (e.g., sensitive) should be considered to reflect the definition found in a commonly accepted dictionary.

note the privacy and security requirements addressed in this Memorandum apply to all Federal information and information systems.<sup>8</sup> Breaches subject to notification requirements include both electronic systems as well as paper documents. In short, agencies are required to report on the security of information systems in any format (*e.g.*, paper, electronic, etc.).<sup>9</sup>

In formulating a breach notification policy, agencies must review their existing requirements with respect to Privacy and Security (see Attachment 1). The policy must include existing and new requirements for Incident Reporting and Handling (see Attachment 2) as well as External Breach Notification (see Attachment 3). Finally, this document requires agencies to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information (see Attachment 4).

Within the framework set forth in the attachments, agencies may implement more stringent policies and procedures reflecting the mission of the agency. While this framework identifies a number of steps to greatly reduce the risks related to a data breach of personally identifiable information, it is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit, such as:

- reducing the volume of collected and retained information to the minimum necessary;
- limiting access<sup>10</sup> to only those individuals who must have such access; and
- using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

This Memorandum should receive the widest possible distribution within your agency and each affected organization and individual should understand their specific responsibilities for implementing the procedures and requirements. Materials created in response to this Memorandum and attachments should be made available to the public through means determined by the agency, *e.g.*, posted on the agency web site, by request, etc.

Consistent with longstanding policy requiring agencies to incorporate the costs for securing their information systems, all costs of implementing this memorandum, including development,

---

<sup>8</sup> FISMA security requirements apply to Federal information and information systems, including both paper and electronic format.

<sup>9</sup> A plan to review the controls for information systems not previously included in other security reviews must be addressed in the agency's breach notification policy (*e.g.*, timeframe for completion of review, etc.); however, completion of the review for those systems is not required to be finished within the 120-day timeframe for development of the policy.

<sup>10</sup> In this policy, "access" means the ability or opportunity to gain knowledge of personally identifiable information.

implementation, notification to affected individuals, and any remediation activities, will be addressed through existing agency resources of the agency experiencing the breach.

Because of the many alternate ways to implement a risk-based program within the framework provided, this Memorandum, or its attachments, should not be read to mean an agency's failure to implement one or more of the many security provisions discussed within<sup>11</sup> would constitute less than adequate protections required by the Privacy Act. These new requirements do not create any rights or benefits, substantive or procedural, which are enforceable at law against the government.

Questions about this Memorandum should be directed to Hillary Jaffe of my staff at [hjaffe@omb.eop.gov](mailto:hjaffe@omb.eop.gov).

Attachments

---

<sup>11</sup> For example, FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST).

**Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information**

This Attachment reemphasizes the responsibilities under existing law, executive orders, regulations, and policy to appropriately safeguard personally identifiable information and train employees on responsibilities in this area (Section A).<sup>12</sup> It also establishes two new privacy requirements and discusses five security requirements as described below (Sections B and C).

**A. Current Requirements**

**1. Privacy Act Requirements.** In particular, the Privacy Act of 1974 (Privacy Act)<sup>13</sup> requires each agency to:

- a. Establish Rules of Conduct. Agencies are required to establish “rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance.” (5 U.S.C. § 552a(e)(9))
- b. Establish Safeguards. Agencies are also required to “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 their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.”<sup>14</sup>
- c. Maintain accurate, relevant, timely and complete information. The Privacy Act also requires personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete including through the use of notices to the public.<sup>15</sup> It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and

---

<sup>12</sup> This Memorandum, or its attachments, should not be read to mean an agency’s failure to implement one or more of the many provisions of FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST) would constitute less than adequate protections required by the Privacy Act of 1974.

<sup>13</sup> 5 U.S.C. § 552a.

<sup>14</sup> 5 U.S.C. § 552a (e)(10).

<sup>15</sup> The Privacy Act requires agencies to “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination” in their systems of records. 5 U.S.C. § 552a(e)(5).

OMB's implementing policies.<sup>16</sup> By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.

## 2. Security Requirements.

Below are four particularly important existing security requirements agencies already should be implementing:

a. Assign an impact level to all information and information systems. Agencies must follow the processes outlined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize all information and information systems according to the standard's three levels of impact (*i.e.*, low, moderate, or high). Agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

b. Implement minimum security requirements and controls. For each of the impact levels identified above, agencies must implement the minimum security requirements and minimum (baseline) security controls set forth in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, respectively.

c. Certify and accredit information systems. Agencies must certify and accredit (C&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.<sup>17</sup> The specific procedures for conducting C&A are set out in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and include guidance for continuous monitoring of certain security controls. Agencies' continuous monitoring should assess a subset of the management, operational, and technical controls used to safeguard such information (*e.g.*, Privacy Impact Assessments).

d. Train employees. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to

---

<sup>14</sup>The Privacy Act requires agencies to publish a notice of any new or intended use of information maintained in a system of records in the Federal Register to provide an opportunity for the public to submit comments. 5 U.S.C. § 552a(e)(4). Agencies are also required to publish notice of any subsequent substantive revisions to the use of information maintained in the system of records. 5 U.S.C. § 552a(e)(11). OMB Circular A-130 ("Management of Federal Information Resources") offers additional guidance on this issue. OMB Circular A-130, App. I, sec. 4.c.

<sup>17</sup> 44 U.S.C. 3544(b).



ensure employees continue to understand their responsibilities.<sup>18</sup> Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing tele-work and other authorized remote access programs, training must also include the rules of such programs.<sup>19</sup>

## **B. Privacy Requirements**

### **1. Review and Reduce the Volume of Personally Identifiable Information.**

a. Review Current Holdings. Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.<sup>20</sup> Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual report under FISMA.

Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act systems of records notices.

To help safeguard personally identifiable information, agencies are reminded they must meet the requirements of FISMA and associated policies and guidance from the OMB and NIST.<sup>21</sup> FISMA requires each agency to implement a comprehensive security program to protect the agency's information and information systems; agency Inspectors General must independently evaluate the agency's program; and agencies must report annually to OMB and Congress on the effectiveness of their program.

---

<sup>18</sup> Agencies may schedule training to coincide with existing activities, such as ethics training. Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. The Department of Defense, the Office of Personnel Management, and the Department of State offer agencies a minimum baseline of security awareness training as part of the Information Systems Security Line of Business.

<sup>19</sup> Agencies should also consider augmenting their training by using creative methods to promote daily awareness of employees' privacy and security responsibilities, such as weekly tips, mouse pads imprinted with key security reminders, privacy screens for public use of laptops, and incentives for reporting security risks.

<sup>20</sup> To the extent agencies are substantively performing these reviews, agencies should leverage these efforts to meet the new privacy requirements. This provision does not apply to apply to the accessioned holdings (archival records) held by the National Archives and Records Administration (NARA).

<sup>21</sup> The Department of Defense and Intelligence Community establish their own policy and guidance for the security of their information systems. 44 U.S.C. 3543(c).



Within the above framework, agencies may implement more stringent procedures governed by specific laws, regulations, and agency procedures to protect certain information, for example, taxpayer data, census information, and other information.

## 2. Reduce the Use of Social Security Numbers.

a. Eliminate Unnecessary Use. Agencies must now also review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.<sup>22</sup>

b. Explore Alternatives. Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (*e.g.*, surveys, data calls, etc.).

## C. Security Requirements

While agencies continue to be responsible for implementing all requirements of law and policy, below are five requirements<sup>23</sup> agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, *e.g.*, law enforcement information, etc.

- Encryption. Encrypt, using only NIST certified cryptographic modules,<sup>24</sup> all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary<sup>25</sup> or a senior-level individual he/she may designate in writing;
- Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a “time-out” function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and

<sup>22</sup> Agencies with questions addressing this assignment regarding the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) should contact their respective desk officer at the Office of Management and Budget.

<sup>23</sup> See OMB Memo 06-16 “Protection of Sensitive Agency Information” ([www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf)).

<sup>24</sup> See NIST’s website at <http://csrc.nist.gov/cryptval/> for a discussion of the certified encryption products.

<sup>25</sup> Non cabinet agencies should consult the equivalent of a Deputy Secretary.

8

- Ensure Understanding of Responsibilities. Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities.

Agencies should also contemplate and incorporate best practices to prevent data breaches. Examples of such practices might include using privacy screens when working outside the office or requiring employees to include laptop computers in carry-on luggage rather than checked baggage.

**Attachment 2: Incident Reporting and Handling Requirements**

This Attachment applies to security incidents involving the breach of personally identifiable information whether in electronic or paper format. For the purposes of reporting, agencies must continue to follow existing requirements, as modified and described below.

**A. Existing Requirements****1. FISMA Requirements.** FISMA requires each agency to:

- implement procedures for detecting, reporting and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done
- 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
  - any other agency or office in accordance with law or as directed by the President.<sup>26</sup>
- implement NIST guidance and standards<sup>27</sup>

Federal Information Processing Standards Publication 200 (FIPS 200) and NIST Special Publication 800-53 provide a framework for categorizing information and information systems, and provide minimum security requirements and minimum (baseline) security controls for incident handling and reporting. The procedures agencies must already use to implement the above FISMA requirements are found in two primary guidance documents: NIST Special Publication 800-61, *Computer Security Incident Handling Guide*<sup>28</sup>; and the concept of operations for the Federal security incident handling center located within the Department of Homeland Security, *i.e.*, United States Computer Emergency Readiness Team (US-CERT).<sup>29</sup>

---

<sup>26</sup> 44 U.S.C. § 3544(b)(7).

<sup>27</sup> For additional information on NIST guidance and standards, see [www.nist.gov](http://www.nist.gov).

<sup>28</sup> See "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology" (<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>).

<sup>29</sup> The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546. Its complete set of operating procedures may be found on the US-CERT website ([www.us-cert.gov/federal/reportingRequirements.html](http://www.us-cert.gov/federal/reportingRequirements.html)). Separate procedures are in place for the Department of Defense as identified in Directive O-8530-1 and all components report incidents to the Joint Task Force Global Network Operations (JTF-GNO), which, in turn, coordinates directly with the US-CERT.

**2. Incident Handling and Response Mechanisms.** When faced with a security incident, an agency must be able to respond in a manner protecting both its own information and helping to protect the information of others who might be affected by the incident. To address this need, agencies must establish formal incident response mechanisms. To be fully effective, incident handling and response must also include sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies. In addition to training employees on how to prevent incidents, all employees must also be instructed in their roles and responsibilities regarding responding to incidents should they occur.

#### **B. Modified Agency Reporting Requirements**

**1. US-CERT Modification.** Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The US-CERT concept of operations for reporting Category 1 incidents is modified as follows:

Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred. Reporting to US-CERT is required within one hour of discovery/detection.

- For incidents involving personally identifiable information, agencies must:
  - Continue to follow internal agency procedures for notifying agency officials including your agency privacy official and Inspector General;
  - Notify the issuing bank if the breach involves government-authorized credit cards; and
  - Notify US-CERT within one hour. Although only limited information about the breach may be available, US-CERT must be advised so it can assist in coordinating communications with the other agencies. Updates should be provided as further information is obtained.
- Under specific procedures established for these purposes, after notification by an agency, US-CERT will notify the appropriate officials.
- Monthly, US-CERT will distribute to designated officials in the agencies and elsewhere, a report identifying the number of confirmed breaches of personally identifiable information and will also make available a public version of the report.

#### **2. Develop and Publish a Routine Use.**

a. Effective Response. A federal agency's ability to respond quickly and effectively in the event of a breach of federal data is critical to its efforts to prevent or minimize any consequent

harm.<sup>30</sup> An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by federal agencies and is subject to the Privacy Act (5 U.S.C. § 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory exceptions.<sup>31</sup> In order to ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C. § 552a(b)(3) of the Privacy Act, agencies should publish a routine use for appropriate systems specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a data breach as follows:

To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.<sup>32</sup>

As described in the President's Identity Theft Task Force's Strategic Plan, all agencies should publish a routine use for their systems of records allowing for the disclosure of information in the course of responding to a breach of federal data.<sup>33</sup> Such a routine use will serve to protect the interests of the individuals whose information is at issue by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harm resulting from a compromise of data maintained in their systems of records.

---

<sup>30</sup> Here, "harm" means damage, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.

<sup>31</sup> 5 U.S.C. §§ 552a(b)(1)-(12).

<sup>32</sup> See Appendix B of the Identity Theft Task Force report ([www.identitytheft.gov/reports/StrategicPlan.pdf](http://www.identitytheft.gov/reports/StrategicPlan.pdf)).

<sup>33</sup> *Id.*



**Attachment 3: External Breach Notification**

To ensure consistency across government, this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification.<sup>34</sup> This Attachment does not attempt to set a specific threshold for external notification since breaches are specific and context dependant and notification is not always necessary or desired. The costs of any notifications must be borne by the agency experiencing the breach from within existing resources.

**A. Background**

**1. Harm.** Breaches can implicate a broad range of harms to individuals, including the potential for identity theft; however, this Section does not discuss actions to address possible identity theft or fraud. Agencies are referred to the ID Theft Task Force's Strategic Plan for guidance.

**2. Requirement.** Agencies must implement the one specific new requirement discussed below; *i.e.*, develop a breach notification policy and plan (see Section B. below).

**3. Threshold questions.** Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies to resolve a number of threshold questions.<sup>35</sup> The likely risk of harm and the level of impact will determine when, what, how and to whom notification should be given.<sup>36</sup>

Notification of those affected and/or the public allows those individuals the opportunity to take steps to help protect themselves from the consequences of the breach. Such notification is also consistent with the "openness principle" of the Privacy Act that calls for agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.

**4. Chilling Effects of Notices.** A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public.<sup>37</sup> In addition, agencies should

---

<sup>34</sup> These factors do not apply to an agency's notification to US-CERT. Agencies must report all incidents – potential and confirmed – involving personally identifiable information to US-CERT.

<sup>35</sup> Notice may not be necessary if, for example, the information is properly encrypted because the information would be unusable.

<sup>36</sup> See OMB's September 20, 2006 memorandum titled "Recommendations for Identity Theft Related Data Breach Notification" for information and recommendations for planning and responding to data breaches which could result in identity theft ([www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf)).

<sup>37</sup> Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10. In this testimony, the Federal Trade Commission raised concerns about the threshold for which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects.

consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.

#### **B. New Requirement**

Each agency should develop a breach notification policy and plan comprising the elements discussed in this Attachment. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notification.

Six elements should be addressed in the policy and plan and when considering external notification:

- whether breach notification is required
- timeliness of the notification
- source of the notification
- contents of the notification
- means of providing the notification
- who receives notification: public outreach in response to a breach

To ensure adequate coverage and implementation of the plan, each agency should establish an agency response team including the Program Manager of the program experiencing the breach, Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy, Communications Office, Legislative Affairs Office, General Counsel and the Management Office which includes Budget and Procurement functions.<sup>38</sup> A more detailed description of these elements is set forth below:

#### **1. Whether Breach Notification is Required**

To determine whether notification of a breach is required, the agency should first assess the likely risk of harm caused by the breach and then assess the level of risk. Agencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.<sup>39</sup> Agencies should bear in mind that notification when there is little or no risk of harm might create

---

<sup>38</sup> Non-Cabinet-level agencies should include their functional equivalent.

<sup>39</sup> For reference, the express language of the Privacy Act requires agencies to consider a wide range of harms: agencies shall "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 their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a (e)(10).

unnecessary concern and confusion.<sup>40</sup> Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Five factors should be considered to assess the likely risk of harm:

a. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals.<sup>41</sup> It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context.<sup>42</sup> In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

b. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification.

c. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the agency. (See Attachment 1 above.) If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent.<sup>43</sup>

Agencies will first need to assess whether the personally identifiable information is at a low, moderate, or high risk of being compromised. The assessment should be guided by NIST

---

<sup>40</sup> Another consideration is a surfeit of notices, resulting from notification criteria which are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant.

<sup>41</sup> For example, theft of a database containing individuals' names in conjunction with Social Security numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

<sup>42</sup> For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.

<sup>43</sup> In this context, proper protection means encryption has been validated by NIST.



security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

d. Likelihood the Breach May Lead to Harm

1. *Broad Reach of Potential Harm.* The Privacy Act requires agencies to 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.”<sup>44</sup> Additionally, agencies should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

2. *Likelihood Harm Will Occur.* The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother’s maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force.<sup>45</sup>

e. Ability of the Agency to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken.<sup>46</sup> Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

---

<sup>44</sup> 5 U.S.C. § 552a(e)(10).

<sup>45</sup> See “Recommendations for Identity Theft Related Data Breach Notification” ([www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf)).

<sup>46</sup> For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

## **2. Timeliness of the Notification**

Agencies should provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement and national security and any measures necessary for your agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Decisions to delay notification should be made by the Agency Head or a senior-level individual he/she may designate in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

## **3. Source of the Notification**

In general, notification to individuals affected by the breach should be issued by the Agency Head, or senior-level individual he/she may designate in writing, or, in those instances where the breach involves a publicly known component of an agency, such as the Food and Drug Administration or the Transportation Security Administration, the Component Head. This demonstrates it has the attention of the chief executive of the organization. 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 or Senior Agency Official for Privacy. This approach signals the agency recognizes both the security and privacy concerns raised by the breach.

When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring any notification and corrective actions are taken. The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

## **4. Contents of the Notification**

The notification should be provided in writing and should be concise, conspicuous, plain language. The notice should include the following elements:

- 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 personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system;
- What steps individuals should take to protect themselves from potential harm, if any;
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

Given the amount of information required above, you may want to consider layering the information as suggested in Section 5 below, providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on your web site. If you have knowledge the affected individuals are not English speaking, notice should also be provided in the appropriate language(s). You may seek additional guidance on how to draft the notice from the Federal Trade Commission, a leader in providing clear and understandable notices to consumers, as well as from communication experts who may assist you in designing model notices.<sup>47</sup> A standard notice should be part of your approved breach plan.

#### **5. Means of Providing Notification**

The best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notice which may be considered.

a. 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.

---

<sup>47</sup> Additional guidance on how to draft a notice is available in the FTC publication titled "Dealing with a Data Breach" ([www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html)). Although the brochure is designed for private sector entities that have experienced a breach, it contains sample notice letters that could also serve as a model for federal agencies. You may also seek guidance from communications experts who may assist you in designing model notices.

b. First-Class Mail. First-class mail notification to the last known mailing address of the individual in your agency's records should be the primary means notification is provided. Where you have reason to believe the address is no longer current, you should take reasonable steps to update the address by consulting with other agencies such as the US Postal Service. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency which experienced the breach uses another agency to facilitate mailing (for example, if the agency which suffered the loss consults the Internal Revenue Service for current mailing addresses of affected individuals), care should be taken to ensure the agency which suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents, *e.g.*, "Data Breach Information Enclosed" and should be marked with the name of your agency as the sender to reduce the likelihood the recipient thinks it is advertising mail.

c. E-Mail. E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address to you and has expressly given consent to e-mail as the primary means of communication with your agency, and no known mailing address is available, notification by e-mail may be appropriate. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the agency and [www.U.S.A.gov](http://www.U.S.A.gov)<sup>48</sup> web sites, where the notice may be "layered" so the most important summary facts are up front with additional information provided under link headings.

d. Existing Government Wide Services. Agencies should use Government wide services already in place to provide support services needed, such as USA Services, including toll free number of 1-800-FedInfo and [www.U.S.A.gov](http://www.U.S.A.gov).

e. Newspapers or other Public Media Outlets. Additionally, you may supplement individual notification with placing notifications in newspapers or other public media outlets. You should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

f. Substitute Notice. Substitute notice in those instances where your agency does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of your agency's web site and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

---

<sup>48</sup> The current domain name for the Federal Internet portal required by section 204 of the E-Government Act of 2002 is [www.usa.gov](http://www.usa.gov).



g. Accommodations. Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the agency web site.

#### **6. Who Receives Notification: Public Outreach in Response to a Breach**

a. Notification of Individuals. The final consideration in the notification process when providing notice is to whom you should provide notification: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification.

b. Notification of Third Parties including the Media. If communicating with third parties regarding a breach, agencies should consider the following.

1. *Careful Planning.* An agency's decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above in Section 2. To the extent possible, when necessary prompt public media disclosure is generally preferable because delayed notification may erode public trust.

2. *Web Posting.* Agencies should post information about the breach and notification in a clearly identifiable location on the home page of your agency web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process.<sup>49</sup> The information should also appear on the [www.U.S.A.gov](http://www.U.S.A.gov) web site. You may also consult with GSA's USA Services regarding using their call center.

3. *Notification of other Public and Private Sector Agencies.* Other public and private sector agencies may need to be notified on a need to know basis, particularly those that may be

---

<sup>49</sup> See the FAQ posted by the Department of Veterans Affairs in response to the May 2006 incident for examples of links to identity theft resources and a sample FAQ ([www.usa.gov/veteransinfo.shtml](http://www.usa.gov/veteransinfo.shtml)).

affected by the breach or may play a role in mitigating the potential harms stemming from the breach.<sup>50</sup>

4. *Congressional Inquiries.* Agencies should be prepared to respond to inquiries from other governmental agencies such as the Government Accountability Office and Congress.

c. Reassess the Level of Impact Assigned to the Information. After evaluating each of these factors, you should review and reassess the level of impact you have already assigned to the information using the impact levels defined by the NIST.<sup>51</sup> The impact levels – low, moderate, and high, describe the (worst case) potential impact on an organization or individual if a breach of security occurs.<sup>52</sup>

- **Low:** the loss of confidentiality, integrity, or availability is expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals
- **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.
- **High:** the loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. If agencies appropriately apply the five risk factors discussed in section 1 of this attachment within the fact-specific context, it is likely notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification.

---

<sup>50</sup> For example, a breach involving medical information may warrant notification of the breach to health care providers and insurers through the public or specialized health media, and a breach of financial information may warrant notification to financial institutions through the federal banking agencies.

<sup>51</sup> See FIPS 199 and Attachment 1 of this memorandum. Reassessment is suggested as the context of any breach may alter your original designation.

<sup>52</sup> The determination of the potential impact of loss of information is made by the agency during an information system's certification and accreditation process.

**Attachment 4: Rules and Consequences****A. New Requirement: Rules and Consequences Policy.**

Fairness requires that managers, supervisors and employees be informed and trained regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities. Therefore, it is the responsibility of each agency head to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of personally identifiable information involved. Supervisors also must be reminded of their responsibility to instruct, train and supervise employees on safeguarding personally identifiable information. Agencies should develop and implement these policies in accordance with the agency's respective existing authorities.

As with any disciplinary action, the particular facts and circumstances, including whether the breach was intentional, will be considered in taking appropriate action. Supervisors also should be reminded that any action taken must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement. Supervisors should understand they may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring.

Agencies having questions regarding development of a rules and consequences policy may contact OPM's Center for Workforce Relations and Accountability Policy at (202) 606-2930.

**1. Affected Individuals.** At a minimum, each agency should have a documented policy in place which applies to employees of the agency (including managers), and its contractors, licensees, certificate holders, and grantees.

**2. Affected Actions.** The agency's policy should describe the terms and conditions affected individuals shall be subject to and identify available corrective actions. Rules of behavior and corrective actions should address the following:

- Failure to implement and maintain security controls, for which an employee is responsible and aware, for personally identifiable information regardless of whether such action results in the loss of control<sup>53</sup> or unauthorized disclosure of personally identifiable information;

---

<sup>53</sup> Here, "control" means the authority of the government agency that originates information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state which may or may not lead to an event, *i.e.*, a breach.

- Exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information;
- Failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and
- For managers, failure to adequately instruct, train, or supervise employees in their responsibilities.

**3. Consequences.** Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. The minimum consequence agencies should consider is prompt removal of authority to access information or systems from individuals who demonstrates egregious disregard or a pattern of error in safeguarding personally identifiable information.



## Appendix B - OMB M-07-04 ("Use of Credit Monitoring Services Blanket Purchase Agreements (BPA)")

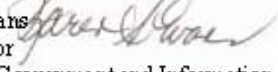


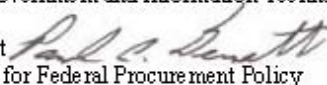
EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

December 22, 2006

M-07-04

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Karen S. Evans   
Administrator  
Office of E-Government and Information Technology

Paul A. Denett   
Administrator for Federal Procurement Policy

SUBJECT: Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)

The purpose of this memorandum is to alert you to the recent establishment of government-wide blanket purchase agreements (BPAs) for commercial credit monitoring services and encourage agency consideration of these vehicles to the maximum extent practicable.

Loss of certain types of personal information and data can lead to identity theft and financial loss. To help protect affected individuals if their personally identifiable information has been lost or stolen, credit monitoring services may be utilized when the agency has determined that mitigation efforts, including credit monitoring, are required to mitigate potential damage due to a data security breach. To assist in making these determinations, agencies should follow the recommendations developed by the President's Identity Theft Task Force and provided in OMB's September 20, 2006 memorandum "Recommendations for Identity Theft Related Data Breach Notification."

The General Services Administration (GSA), under the direction of OMB, is leading and managing a credit monitoring services initiative. This initiative includes the establishment of BPAs against Federal Supply Schedule contracts to provide the government a fast and effective way to order commercial credit monitoring services. This initiative will leverage the government's spending power by offering reduced prices and enable improved oversight and better reporting.

The BPAs offer a variety of protection levels, depending on the degree of risk, vulnerability, and exposure encountered, and supports a consistent approach to mitigating the adverse impacts of personal data loss. The BPAs do not obligate funds and the government is obligated only to the extent that authorized task orders are issued under the BPA. There is no limit on the dollar value of task order purchases made under the BPA, and the period of performance of the GSA BPAs will not exceed five years.

When a new requirement for credit monitoring services arises, agencies shall review the pricing and terms and conditions of the GSA BPAs, in addition to any other credit monitoring services they may be considering in their market research. Procedures for placing orders on the BPAs are set forth in Attachment 1. If an agency decides to acquire credit monitoring services other than through the GSA BPAs, the agency shall send a notification to GSA, with a copy to the OMB E-Government Administrator, explaining how the proposed contract offers a better value to the agency. Access to this information will allow GSA to review the BPAs and ensure they offer best value credit monitoring services. Accordingly, the notice should identify the pricing and terms and conditions of the award. Notices shall be prepared in coordination with the agency's Office of the Chief Acquisition Officer and the Office of the Chief Information Officer and submitted at least 10 days prior to making an award, except in the event of unusual and compelling urgency, in which case the notice shall be provided as soon as practicable.

Please address any questions regarding the use of the GSA BPA to Mr. Houston Taylor, Director of GSA's Services Acquisition Center, at (703) 605-2688.

Attachment

cc: Chief Acquisition Officers  
Chief Information Officers  
Chief Financial Officers  
Chief Human Capital Officers

Attachment 1

**Credit Monitoring Services  
Blanket Purchase Agreement Information**

**Government Points of Contact**

U.S. General Services Administration  
Crystal Plaza 4, 2200 Crystal Drive, 7<sup>th</sup> Floor  
Arlington, VA 22202

BPA Contracting Officer  
Houston Taylor  
E-mail: [houston.taylor@gsa.gov](mailto:houston.taylor@gsa.gov)

Alternate:  
Dennis Harrison  
E-mail: [dennis.harrison@gsa.gov](mailto:dennis.harrison@gsa.gov)

**Website**  
[www.gsaadvantage.gov/strategicsourcing](http://www.gsaadvantage.gov/strategicsourcing)

**BPA Holders***Bearak Reports*

BPA #: GS-23F-A0013  
MAS Contract#: GS-23F-0125S  
Date of Award: 14-Aug-06  
Address: 1257 Worcester Road Suite 308  
Framingham, MA 01701  
POC: Judith Leary: [judy@bearak.com](mailto:judy@bearak.com) or [jleary@bearak.com](mailto:jleary@bearak.com)

*Equifax Inc.*

BPA #: GS-23F-A0014  
MAS Contract #: GS-22F-9663D  
Date of Award: 14-Aug-06  
Address: 1550 Peachtree Street, NW  
Atlanta, Georgia 30309  
POC: Melissa Thomas: [melissa.thomas@equifax.com](mailto:melissa.thomas@equifax.com)

*Experian Consumer Direct*

BPA #: GS-23F-A0015  
MAS Contract #: GS-23F-0356P  
Date of Award: 14-Aug-06  
Address: 18500 Von Karman Avenue Suite 900  
Irvine, CA 92612  
POC: Tim Olson: [tim.olson@experian.com](mailto:tim.olson@experian.com)

**Ordering Procedures**

In accordance with Federal Acquisition Regulation (FAR) 8.405-3 GSA, in partnership with any ordering agency, will establish multiple BPAs with Federal Supply Schedule (FSS) contract holders.

- (a) *General.* Any ordering agency shall use the procedures in this subsection when ordering services priced at hourly rates as established by the FABS Schedule contracts. The applicable services shall be Special Item Numbers (SIN) 520 16 Business Information Services.
- (b) *Statement of Work (SOW).* Any ordering agency shall prepare SOWs that include, at a minimum, work to be performed, location of work, period of performance, deliverable schedule, applicable performance standards, and any special requirements.
- (c) *Request for Quotation (RFQ) procedures.* Any ordering agency shall provide the RFQ to include at a minimum the SOW and evaluation criteria.
  - 1) *Orders at or below the micro purchase threshold.*
    - (i) Any ordering agency may place orders at or below the micro-purchase threshold (\$2500) with any BPA-holder. Any ordering agency should attempt to distribute orders at or below the micro-purchase threshold among all BPA holders.
  - 2) *Orders exceeding the micro-purchase threshold.*
    - (i) Any ordering agency shall develop an SOW in accordance with the instructions stated in paragraph (b) above.
    - (ii) Any ordering agency shall provide the RFQ (including SOW and evaluation criteria) to at least three BPA-holders.
    - (iii) Any ordering agency shall request that BPA-holders submit firm-fixed prices to perform services identified in the SOW. This does not preclude the use of Labor Hour or Time and Material (T&M) task orders.
  - 3) *Orders exceeding the maximum order threshold of \$1,000,000.*
    - (i) Any ordering agency shall provide the RFQ (including SOW and evaluation criteria) to additional BPA-holders. When determining the appropriate number of BPA-holders, any ordering agency may consider, among other factors, the following:
      - A. The complexity, scope and estimated value of the requirement.
      - B. The market search results.
    - (ii) Seek price reductions.
  - 4) Any ordering agency shall provide the RFQ (including the SOW and evaluation criteria) to any BPA-holder that requests a copy of it.
- (d) *Evaluation.* Any ordering agency shall evaluate all responses received using the evaluation criteria provided to the BPA-holders. Any ordering agency is responsible for considering the level of effort and the mix of labor proposed to perform specific tasks being ordered, and for determining that the total price is reasonable. Place the task order with the BPA-holder that represents the best value (see FAR 8.404 (d)). After award any ordering agency shall provide timely notification to unsuccessful BPA-holders. If an unsuccessful BPA-holder requests information on an award that was based on factors other than price alone, a brief explanation of the basis for the award decision shall be provided.

- (e) *Minimum documentation.* Any ordering agency shall document:
- 1) The BPA-holders considered, noting the BPA-holder from which the service was purchased;
  - 2) A description of the service purchased;
  - 3) The amount paid;
  - 4) The evaluation methodology used in selecting the BPA-holder to receive the task order;
  - 5) The rationale for any tradeoffs in making the selection;
  - 6) The price reasonableness determination required by paragraph (d) of this subsection; and
  - 7) The rationale for using other than—
    - (i) A firm-fixed price task order; or
    - (ii) A performance-based task order.

## Appendix C: Federal Trade Commission Links

In addition to a letter informing the data subject(s) of the breach, the PO may also want to include information from the FTC about responses to identity theft. It is recommended that the most current information be attached to the external breach notification letter to help breach subjects understand their options and where they can go for more information.

The link to the FTC consumer identity theft webpage is:

<http://www.ftc.gov/bcp/menus/consumer/data/idt.shtm>.

The link to the FTC identity theft information webpage is:

<http://www.ftc.gov/bcp/online/pubs/credit/idcrisis.shtm>.