

UNITED STATES  
DEPARTMENT OF THE INTERIOR  
BUREAU OF LAND MANAGEMENT  
ARIZONA STATE OFFICE SUPPLEMENT  
MANUAL TRANSMITTAL SHEET

Release  
1-160

Date  
AUG - 6 2010

Subject

1278 - Access to Privacy Information and Records

1. Explanation of Material Transmitted: Arizona State Office, BLM Manual Supplement - "Safeguarding Privacy Information"
2. Reports Required: None
3. Material Superseded: Information Bulletin and Instruction Memorandum noted below.
4. Filing Instructions: File in BLM Manual 1278 as directed below.

REMOVE

IB - AZ-2005-014  
IM - AZ-2007-023

INSERT

MS-1278-AZ-1, Rel. 1-160

*Fon*  
  
James G. Kenna, State Director

**I – PURPOSE AND OBJECTIVES ..... 1**

**II – RESPONSIBILITIES**

**A. Line Officials..... 1**

**B. Supervisors ..... 1**

**C. State Privacy Specialist ..... 1**

**D. State Employee and Labor Relations Specialist ..... 1**

**E. State Information Technology Security Specialist ..... 1**

**D. All AZ Employees ..... 2**

**III – POLICY AND PROCEDURES**

**A. General Policy ..... 2**

**B. Privacy Act ..... 2**

**C. Personally Identifiable Information (PII) ..... 3**

**D. Procedures**

    1. Case Files ..... 3

    2. E-mail Messages ..... 4

    3. Work Papers ..... 4

    4. BLM Employee Forms/Information ..... 4

**IV – PRIVACY VIOLATIONS**

**A. Reporting Violations ..... 5**

**B. Procedures ..... 5**

**C. Additional OMB Requirements ..... 6**

**Appendices**

Appendix A – Steps to Safeguarding Privacy Information ..... 7

Appendix B – Table of Offenses and Penalties ..... 8

Appendix C – Restricted Access "Notice!" ..... 9

Appendix D – BLM Form S-137 – *Privacy "WARNING" Notice* ..... 10

Appendix E – Privacy Act 5 U.S.C. 552a (Excerpts) ..... 11-12

Appendix F – Privacy Act 43 CFR Part 2, Subpart B (Excerpts) ..... 13-14

**AZ Manual Supplement 1278 – SAFEGUARDING PRIVACY INFORMATION – (Public)**

TC-2

Appendix G – BLM Form 1273-2 - *Proprietary/Confidential Information* ..... 15-16  
Appendix H – Form AZ-1278-15 - *Privacy Violation Notification and Action* .....17  
Appendix I – OMB Memorandum M-07-16..... 18-39

## I. PURPOSE AND OBJECTIVES

This Manual Supplement (MS) contains policy for all Arizona (AZ) offices of the Bureau of Land Management (BLM) regarding the protection of Personally Identifiable Information (PII) and other privacy information. The objectives are to inform all employees of the policies for safeguarding PII and other privacy information and to provide procedures for implementing those safeguards and actions to take when a breach occurs. This MS complies with the Office of Management and Budget (OMB) instructions to all Federal agencies contained in OMB Memorandum M-07-16 – *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (Appendix I).

## II. RESPONSIBILITIES

- A. **Line Officials** - Line Officials (State Director/Associate State Director, Deputy State Directors, District Managers/Associate District Managers, and Field Managers) are responsible for policy awareness and implementation within their offices, ensuring that employees are informed of their responsibilities and requirements for protecting privacy information.
- B. **Supervisors** - Supervisors are responsible for ensuring their employees are aware of the requirements for safeguarding PII and other privacy information, are instructed in the mechanics of implementing safeguards (i.e., how to encrypt e-mail messages on the BLM system), and for verifying that employees complete the required annual Privacy Training on-line course by the due date. Upon notification of a privacy violation, Supervisors are required to conduct informal investigations into the incident and take appropriate action with the liable employee to correct the behavior that caused the violation.
- C. **State Privacy Specialist** - The State Privacy Specialist is responsible for development and maintenance of AZ specific privacy policies; for the maintenance and distribution of BLM, Department of the Interior (DOI), and OMB policies relating to privacy information; and for advising Line Officials, Supervisors, and employees to resolve privacy questions and incidents.
- D. **State Employee and Labor Relations Specialist** - When it is determined that disciplinary action is required, it is the State Employee and Labor Relations Specialist's responsibility to provide guidance and assistance to Supervisors and Line Officials to determine and implement appropriate action(s).
- E. **State Information Technology (IT) Security Specialist** - The IT Security Specialist is often the first recipient of notifications (in the form of "Help Desk tickets") when an incident occurs that involves the BLM's computer or e-mail systems. It is the State IT Security Specialist's responsibility to promptly determine if any privacy-related information is involved and, if it is, to immediately notify the State Privacy Specialist for appropriate action.

- F. **All AZ Employees** - It is the responsibility of every employee to protect their own privacy information and to safeguard any individual's PII they may possess or obtain in the course of doing business. (See Appendix A - *Steps to Safeguarding Privacy Information*.) All employees are responsible for promptly reporting all privacy violations which they observe or have first-hand knowledge of.

### III. POLICY AND PROCEDURES

#### A. **General Policy**

1. Information subject to the Privacy Act, PII, or other privacy data contained in BLM records (including forms and e-mail messages) must be properly safeguarded to ensure that personal privacy information is not disclosed to others.
2. Every employee must be familiar with requirements for safeguarding PII and other privacy information and be aware of the consequences of both inadvertent and intentional breaches. Inadvertent violations are subject to counseling and training requirements explained in this MS at Section IV (B). Intentional violations are subject to disciplinary actions prescribed in the DOI Manual 370 DM 752 (see Appendix B for privacy-related excerpts).

#### B. **Privacy Act**

1. The Privacy Act (5 U.S.C. 552a) protects personal information maintained in groups of records/files (known as "a system of records") that are retrieved by a personal identifier (i.e., a name, Social Security Number, or other unique personal identifier). This means the group of records/files are organized, stored, and retrieved by that personal identifier, and/or when electronic information can be sorted and retrieved by that personal identifier. The Privacy Act only applies to those types of systems of records. However, not all privacy information is protected by the Privacy Act, because not all PII or other privacy data is maintained in a system where records are retrieved in this manner.
2. Records protected by the Privacy Act are required to have a current System of Records Notice (SORN) which has been published in the *Federal Register* to notify the public (and employees) of the collection of personal information.
3. Information contained in a Privacy Act system of records may not be disclosed to others unless written permission is obtained from the subject of the records, or disclosure is authorized as stated in the SORN for those records.
4. Privacy Act records should contain a restricted access "Notice" (Appendix C) and are required to be stored in locked metal cabinets or locked rooms also labeled with a BLM Form S-137 (Appendix D) or equivalent notice.

5. Additional requirements of the Privacy Act are provided in Appendix E (excerpts from 5 U.S.C. § 552a) and Appendix F (43 CFR §§ 2.51 and 2.52).

**C. Personally Identifiable Information**

1. PII is "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity such as their name, Social Security Number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual" (OMB Memorandum M-06-19).
2. PII can be in any BLM record, including forms and e-mail messages, and includes any personal or sensitive information about individual members of the public and/or BLM employees. Additional examples of PII include, but are not limited to:
  - a. Home addresses, personal e-mail addresses, and personal telephone/cell phone/pager numbers.
  - b. Personal identifiers such as driver's license numbers, personal vehicle license numbers, and credit card numbers (including Government-issued credit cards).
  - c. Age, other names used, marital status, race and/or ethnic background, party or union affiliation, and financial information.

**D. Procedures**

1. Case Files:
  - a. Privacy information maintained within a case file must be separated from other records in the file.
  - b. Privacy records should be placed in a blue envelope, or a pocket folder, with a BLM Form 1273-2 (Appendix G) stapled to the front and kept in the case file.
  - c. The clearly marked blue envelope/pocket folder must be removed from the file and kept in a secure place when anyone from the public views the file and returned to the case file following the review.

2. E-mail Messages:

- a. E-mail messages should not include PII or privacy information in them. E-mail announcements of events, such as a birth or death, should never include the home address and/or phone number of family members; instead provide a contact name in the office where that information can be obtained.
- b. If a BLM business function requires the e-mail transmittal of any privacy information, the message must be sent using the "encryption" function in the e-mail system. (Note: Currently, encrypted messages can only be sent between BLM offices.)
- c. If privacy information needs to be transmitted to someone outside BLM, remove the privacy information from the message and inform the recipient that the privacy information will be sent separately via a secured facsimile (fax). (Note: The fax transmittal sheet should be properly marked to alert the recipient of the need to protect the information.)
- d. Receipt of an e-mail message and its attachments that contains PII or other privacy information **must not** be forwarded to others, unless encrypted. Knowingly forwarding PII or privacy information may be considered a willful release of privacy information.

3. Work Papers:

- a. Documents containing PII and privacy information must be safeguarded in offices and work areas to avoid exposure to anyone who does not have a "need to know." When authorized employees leave their work area (e.g., lunch, break, etc.) all privacy-protected documents must be secured.
- b. Leaving privacy information unsecured on a computer screen, desk, copier, or fax machine is a release of that information and should be reported as a privacy violation.

4. BLM Employee Forms/Information:

- a. Employees are not required to provide personal information on any form that does not contain the proper authorization for collecting personal information. Forms must contain a notice clearly stating the authority for collecting any privacy information, the intended use of the information, where the information will be stored, and who will have access to it. (Note: Privacy information on a BLM form may **only** be used by Supervisors, Line Officials, and authorized employees for the purpose(s) stated on the form; any other use is a privacy violation.)

- b. Employees should verify that any requested PII is actually required before providing such information. (For example: Some forms have traditionally collected Social Security Numbers, but there may no longer be a need for this; e.g., OPM Form 71 - Request for Leave or Approved Absence is no longer submitted to Payroll but instead remains with the local timekeeper, so there is no need to put a Social Security Number on this form.)
- c. Distribution of employee forms or other documents containing any PII (i.e., personnel forms, requests for leave, credit card statements, travel vouchers, etc.) must be distributed in a blue envelope.

#### IV. PRIVACY VIOLATIONS

##### A. Reporting Violations

1. Privacy breach incidents may initially be reported to a Supervisor, Line Official, a Human Resources Specialist, or directly to the State Privacy Specialist. In addition, the DOI and BLM Washington Office (WO) continuously monitor and audit use of the e-mail system and the Internet for privacy violations and incidents are often first reported to the State IT Security Specialist.
  - a. Immediately inform the State Privacy Specialist of the incident to initiate required action. Details of the incident may be submitted via an encrypted e-mail message, a phone call, or a secured fax to the State Privacy Specialist (AZ-9540).

##### B. Procedures

1. The State Privacy Specialist establishes a case file for the violation and prepares a Form AZ-1278-15 – *Privacy Violation Notification and Action* (Appendix H), assigning a due date two weeks from the date of notification. If additional time is needed, extensions may be requested and granted via e-mail message. (Note: Obtain the current version of Form AZ-1278-15 from the AZ website.)
2. By encrypted e-mail, the State Privacy Specialist sends a scanned copy of the Form AZ-1278-15 to the responsible Field Manager/Deputy State Director (FM/DSD) where the violation occurred. (Note: The overseeing Line Official and the WO Privacy Officer are "courtesy copied" this notification for informational purposes only.)
3. The FM/DSD assigns the Form AZ-1278-15 to the responsible Supervisor who promptly conducts an informal investigation of the incident, documents the findings, and reports the results to their Line Official. Appropriate action is determined between the Supervisor and their Line Official, consulting with the State Privacy Specialist, State Employee and Labor Relations Specialist, and/or the State Human Resources Officer, as needed.

- a. *Inadvertent violations* require the Supervisor to counsel the employee about their responsibilities for safeguarding PII and other privacy information by reviewing current policies and ensuring completion of the annual on-line DOI Privacy Training course. At the discretion of the Supervisor and/or Line Official, the employee may be required to re-take the DOI Privacy Training course.
  - b. *Intentional violations* of privacy policies require consultation with the State Human Resources Officer and/or the State Employee and Labor Relations Specialist to determine appropriate disciplinary action. The DOI Disciplinary Manual, 370 DM 752, contains the consequences for intentional violations; see Appendix C for a summary of privacy-related disciplinary actions.
4. Upon completion of all required actions, make notations to Form AZ-1278-15, sign and date the form, and return it to the State Privacy Specialist.
  5. The State Privacy Specialist reports the results to the WO Privacy Officer to close the case or initiate additional action, if the WO deems it is warranted.

**C. Additional OMB Requirements**

Appendix I is the full text of OMB Memorandum M-07-16 – *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. Additional procedures required by this Memorandum fall outside the Privacy Program and are handled by the State IT Security Specialist. Contact the State IT Security Specialist to determine if other procedures are required by that program.

## STEPS TO SAFEGUARDING PRIVACY INFORMATION

Every employee plays an important role in ensuring that Personally Identifiable Information (PII) and other privacy information are protected. Steps to safeguarding privacy include:

1. Do not collect any personal information that is not authorized for collection.
2. Do not distribute or release personal information to anyone who does not have a need for access.
3. Do not send personal information over a fax unless properly marked to alert recipient(s) of the need to protect the information.
4. Encrypt e-mail messages that contain PII and privacy-protected information.
5. Do not commingle privacy information in case files; place all records with privacy or sensitive information in a separate section identified with a Form 1273-2 or other notice.
6. Restrict access to privacy records by storing them in a locked metal file cabinet or in a locked room.
7. Mark all work areas, storage cabinets, and files where protected information is kept with a Form S-137, a Form 1273-2, or other notice.
8. Do not place any PII or other privacy information on the Intranet or Internet.
9. Always use a blue envelope when distributing forms or documents that contain PII or other personal information.
10. If asked to provide personal information over the phone, verify who the caller is to ensure they have a right to the information. (If a BLM employee calls, check the e-mail address book to verify who they are. If it is someone outside BLM, get a phone number and offer to call them back once the need/right is verified.)
11. As organizational and procedural changes occur, think about the privacy implications of current practices. Just because a process has always been done a certain way, does not mean it should continue to be done that way.
12. Respect privacy and be aware of the civil and criminal penalties associated with violations. (See 5 U.S.C. § 552a 3(g) and Departmental Manual 383 DM 9.7.)
13. Always err on the side of caution. If unsure whether certain information is sensitive, presume it is and **protect it**.

## TABLE OF OFFENSES AND PENALTIES

### (Excerpts from 370 DM 752 – DOI Disciplinary Manual)

This Table provides a list of common infractions, along with a suggested range of penalties for each; it does not presume to cover all possible offenses, nor does it mandate the use of specific penalties in most disciplinary situations. The range of penalties described in the Table is intended to serve as a guide to discipline, not a rigid standard . . .

	<b>Nature of Offense (General Misconduct)</b>	<b>Penalty for First Offense</b>	<b>Penalty for Second Offense</b>	<b>Penalty for Third Offense</b>	<b>Remarks</b>
2.	<p>Improper or unauthorized release of sensitive and administratively-controlled information or employee records; failure to safeguard classified material.</p> <p>a. Information is not compromised and release is unintentional.</p> <p>b. Information is compromised and release is unintentional.</p> <p>c. Release of restricted information is deliberate.</p>	<p>Written Reprimand to 5-day suspension</p> <p>Written Reprimand to 30-day suspension</p> <p>30-day suspension to removal</p>	<p>5- to 30-day suspension</p> <p>30-day suspension to removal</p> <p>Removal</p>	<p>30-day suspension to removal</p> <p>Removal</p>	<p>Refer to 5 USC 552a and 43 CFR 2.52 for Privacy Act provisions regarding the misuse of personal information; also refer to 18 USC 798 and 18 USC 1905. Deliberate disclosures of Privacy Act information must be referred to OIG.</p>
12.	<p>Loss, misuse of, damage to or failure to safeguard Government property, records, or information (e.g., willful or negligent damage to Government resources; carelessness in performance of duty resulting in waste of public funds).</p>	<p>Written Reprimand to 14-day suspension</p>	<p>14- to 30-day suspension</p>	<p>30-day suspension to removal</p>	<p>Refer to 5 CFR 2635.101(9). For misuse of Government vehicles, see item 5 under Violations of Statute. Referral to OIG may be appropriate.</p>
32.	<p>Unauthorized use of nonpublic information.</p>	<p>Written Reprimand to removal</p>	<p>Removal</p>		<p>Refer to 5 CFR 2635.703.</p>

# **NOTICE!**

- 1. ACCESS TO THESE RECORDS IS LIMITED TO  
AUTHORIZED PERSONS ONLY!**
  
- 2. INFORMATION MAY NOT BE DISCLOSED FROM THIS  
FILE UNLESS PERMITTED PURSUANT TO  
43 CFR 2.56.**
  
- 3. THESE RECORDS MAY NOT BE ALTERED OR  
DESTROYED EXCEPT AS AUTHORIZED BY  
43 CFR 2.52.**
  
- 4. THE PRIVACY ACT CONTAINS PROVISIONS FOR  
CRIMINAL PENALTIES FOR KNOWINGLY AND  
WILLFULLY DISCLOSING INFORMATION FROM THIS  
FILE UNLESS PROPERLY AUTHORIZED.**

BLM Form S-137 (adhesive label):



**Privacy Act - 5 U.S.C. 552a**

**(e) Agency Requirements** — Each agency that maintains a system of records shall —

**(1)** maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

**(2)** collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

**(3)** inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

**(A)** the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

**(B)** the principal purpose or purposes for which the information is intended to be used;

**(C)** the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

**(D)** the effects on him, if any, of not providing all or any part of the requested information;

**(4)** subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include —

**(A)** the name and location of the system;

**(B)** the categories of individuals on whom records are maintained in the system;

**(C)** the categories of records maintained in the system;

**(D)** each routine use of the records contained in the system, including the categories of users and the purpose of such use;

**(E)** the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

**(F)** the title and business address of the agency official who is responsible for the system of records;

**(G)** the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

**(H)** the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

**(I)** the categories of sources of records in the system;

- (5)** 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;
- (6)** prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;
- (7)** maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;
- (8)** make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;
- (9)** 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 this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;
- (10)** 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;
- (11)** at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and
- (12)** if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

[Code of Federal Regulations]

TITLE 43--PUBLIC LANDS: INTERIOR

PART 2 – Subpart G – Privacy Act

**§ 2.51 Assuring integrity of records.**

(a) *Statutory requirement.* The Privacy Act requires that records subject to the Act be maintained with 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).

(b) *Records maintained in manual form.* When maintained in manual form, records subject to the Privacy Act shall be maintained in a manner commensurate with the sensitivity of the information contained in the system of records. The following minimum safeguards, or safeguards affording comparable protection, are applicable to Privacy Act systems of records containing sensitive information:

(1) Areas in which the records are maintained or regularly used shall be posted with an appropriate warning stating that access to the records is limited to authorized persons. The warning also shall summarize the requirements of § 2.52 and state that the Privacy Act contains a criminal penalty for the unauthorized disclosure of records to which it applies.

(2) During working hours, (i) the area in which the records are maintained or regularly used shall be occupied by authorized personnel or (ii) access to the records shall be restricted by their storage in locked metal file cabinets or a locked room.

(3) During non-working hours, access to the records shall be restricted by their storage in locked metal file cabinets or a locked room.

(4) Where a locked room is the method of security provided for a system, the bureau responsible for the system shall supplement that security by (i) providing lockable file cabinets or containers for the records or (ii) changing the lock or locks for the room so that they may not be opened with a master key. For the purposes of this paragraph, a master key is a key which may be used to open rooms other than the room containing records subject to the Privacy Act, unless those rooms are utilized by officials or employees authorized to have access to the records subject to the Privacy Act.

(c) *Records maintained in computerized form.* When maintained in computerized form, records subject to the Privacy Act shall be maintained, at a minimum, subject to safeguards based on those recommended in the National Bureau of Standard's booklet "Computer Security Guidelines for Implementing the Privacy Act of 1974" (May 30, 1975), and any supplements thereto, which are adequate and appropriate to assuring the integrity of records in the system.

(d) *Office of Personnel Management personnel records.* A system of records made up of Office of Personnel Management personnel records shall be maintained under the security requirements set out in 5 CFR 293.106 and 293.107.

(e) *Bureau responsibility.*

(1) The bureau responsible for a system of records shall be responsible for assuring that specific procedures are developed to assure that the records in the system are maintained with security meeting the requirements of the Act and this section.

(2) These procedures shall be in writing and shall be posted or otherwise periodically brought to the attention of employees working with the records contained in the system.

## **§ 2.52 Conduct of employees.**

(a) *Handling of records subject to the Act.* Employees whose duties require handling of records subject to the Privacy Act shall, at all times, take care to protect the integrity, security and confidentiality of these records.

(b) *Disclosure of records.* No employee of the Department may disclose records subject to the Privacy Act unless disclosure is permitted under § 2.56 or is to the individual to whom the record pertains.

(c) *Alteration of records.* No employee of the Department may alter or destroy a record subject to the Privacy Act unless (1) such alteration or destruction is properly undertaken in the course of the employee's regular duties or (2) such alteration or destruction is required by a decision under §§ 2.70 through 2.75 or the decision of a court of competent jurisdiction.

(d) *Bureau responsibility.* The bureau responsible for a system of records shall be responsible for assuring that employees with access to the system are made aware of the requirements of this section and of 5 U.S.C. 552a(i)(1), which imposes criminal penalties for knowingly and willfully disclosing a record about an individual without the written request or consent of that individual unless disclosure is permitted under one of the exceptions listed in § 2.56 (b) and (c).

UNITED STATES  
DEPARTMENT OF THE INTERIOR  
BUREAU OF LAND MANAGEMENT

# **PROPRIETARY/CONFIDENTIAL INFORMATION**

RECORDS CONTAINED HEREIN  
ARE PROPRIETARY/CONFIDENTIAL  
INFORMATION AND MUST BE  
SAFEGUARDED FROM  
UNAUTHORIZED DISCLOSURE

PROPRIETARY/CONFIDENTIAL INFORMATION

COVER MUST BE ATTACHED TO THE  
RECORD AT ALL TIMES WHEN THE  
RECORD IS REMOVED FROM THE FILES.

## TITLE 18—CRIMES AND CRIMINAL PROCEDURE

### § 1905. Disclosure of confidential information generally

Whoever, being an officer or employee of the United States or of any department or agency thereof, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311-1314), publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined not more than \$1,000, or imprisoned not more than one year, or both; and shall be removed from office or employment.

(June 25, 1948, ch. 645, 62 Stat. 791; Sept. 12, 1980, Pub. L. 96-349 § 7(b), 94 Stat. 1158.)

UNITED STATES DEPARTMENT OF THE INTERIOR  
 BUREAU OF LAND MANAGEMENT  
 Arizona State Office

**PRIVACY VIOLATION NOTIFICATION AND ACTION**

To: \_\_\_\_\_ Date: \_\_\_\_\_  
 (Responsible Manager for Assignment to Supervisor)

From: \_\_\_\_\_  
 State Privacy Specialist (AZ-9540)

Subject: Notification of Privacy-Related Incident – Action Required

Name of Employee: \_\_\_\_\_ Office: \_\_\_\_\_

Date of Incident: \_\_\_\_\_ Description of Incident: \_\_\_\_\_

**Actions Required - Assign to responsible supervisor to complete all of the following:**

- Case-Specific Actions: \_\_\_\_\_
- Verify completion of required on-line Privacy Training; Indicate date completed: \_\_\_\_\_
- Counsel employee on BLM/DOI requirements for safeguarding Personally Identifiable Information (PII) and other Privacy data. Instruct employee to review policies in BLM Manual Supplement, Arizona State Office MS-1786-AZ-1 – Safeguarding Privacy Information.
- Other action(s) deemed necessary by Supervisor or Responsible Manager (may require consultation with State Employee and Labor Relations Specialist). Please describe: \_\_\_\_\_

Signature of Employee	Date
Signature of Supervisor	Date
Signature of Responsible Manager	Date

**NOTE:** Return to State Privacy Specialist (AZ-9540) by Due Date: \_\_\_\_\_

AZ-1278-15  
 08/06/10



**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 trashcan 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 formant (*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 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.

- 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.USA.gov](http://www.USA.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.USA.gov](http://www.USA.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.USA.gov](http://www.USA.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.