Special Attention of

Notice CIO-08-06

Issued September 30, 2008

Expires September 30, 2009

Cross References

Subject

U.S. Department of Housing and Urban Development Breach Notification Policy and Response Plan

This extends the original U.S. Housing and Urban Development Breach Notification Policy and Response Plan (CIO 07-01), issued September 19, 2007.

Distribution: W-3-1,

U.S. Department of Housing and Urban Development
Breach Notification Policy and Response Plan

1-1 Purpose. Federal agencies collect and disseminate personally identifiable information, or PII, during the normal course of conducting business. To retain the trust of the public, business partners, and employees, agencies must safeguard PII by implementing the required physical and operational security requirements and establishing the appropriate policies, procedures, and processes that prevent unauthorized disclosure or access of PII data.

However, even with the best protections in place, unauthorized disclosure or access to PII can still occur. Consequently, the Office of Management and Budget (OMB) Memorandum, M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, requires that HUD develop a comprehensive breach notification policy and plan that addresses the following six elements:

- Whether breach notification is required
- Timeliness of the notification
- Source of the notification
- Contents of the notification
- Means of providing the notification
- Who receive notifications and the public outreach in response to a breach?

This HUD Breach Notification Policy and Response Plan provides Departmental policies and procedures that supplement current requirements for reporting and handling incidents pursuant to the Federal Information Security Management Act of 2002 (FISMA), the Privacy Act of 1974, the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (SP 800-61), and the concept of operations for the United States Computer Emergency Readiness Team (US-CERT).

1-2 Definitions.

A. Personally identifiable information (PII). Refers to information which can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

B. Covered Information. Refers to PII posing a risk of identity theft. Covered information shall, at a minimum, include the following information, whether in paper, in electronic form, or communicated orally:

1. An individual's Social Security Number (SSN) alone; or

2. An individual's name, address, or phone number in combination with one or more of the following:

    a. Date of Birth

    b. SSN

    c. Driver's license number or other state identification number or foreign country equivalent

    d. Passport number

    e. Financial account number

    f. Credit or debit card number

C. Breach. The term used to include the loss of control, compromise, 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 PII and Covered Information, whether physically or electronically.

D. Incident. Same as breach. See above.

E. Access. The ability or opportunity to gain knowledge of PII.

F. Unauthorized Access. An individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.

G. Denial of Service. An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.

H. Malicious Code. Successful installation of malicious software that infects an operating system or application(s).

I. Improper Use. A violation of established computing use policies.

J. Scans, Probes, or Attempted Access. Any activity that seeks to access or identify a federal agency computer, open ports, protocol, service, or any combination for exploitation purposes.

1-3 HUD Breach Notification Response Team

A. The Department has established the HUD Breach Notification Response Team (BNRT) to ensure adequate coverage and implementation of the HUD Breach Notification Policy and Response Plan.

B. Membership. Consistent with OMB Memorandum M-07-16, the Departmental Breach Notification Response Team members shall consist of the following members (or their designees):

1. Chief Information Officer (CIO) / Senior Official for Privacy

   a. The CIO / Senior Official for Privacy shall serve as the Chair for the Breach Notification Response Team, preside over meetings, and initiate responses as appropriate.

   b. The CIO, in coordination with the HUD Computer Security Incident Response Center (HCSIRC), shall take all necessary steps to contain, control, and mitigate the risks from the breach and prevent further unauthorized access to or use of individual information. The CIO shall take these steps without undue delay and consistent with current requirements under FISMA.

2. Chief Information Security Officer (CISO)

   a. The CISO will serve as the Co-chair of the Breach Notification Response Team.

   b. The CISO shall ensure that necessary steps are taken to contain and control a breach and prevent further unauthorized access to or use of individual information. The CISO shall take these steps without undue delay and do so in coordination with the appropriate offices.

3. General Counsel

   The General Counsel shall be responsible for providing legal support and guidance in response to a suspected or actual breach. This responsibility includes but is not limited to:

   a. Determining whether referral of a breach to other authorities is warranted.

   b. Serving as the Department's official legal representative in any formal administrative or judicial proceedings that might arise as a result of a suspected or actual breach.

4. Inspector General (IG)

The IG shall assist with the determination of the risk of harm and the need for providing individuals with notice. In addition, in accordance with the Inspector General Act and other applicable laws, the IG shall conduct an investigation to determine:

a. If the breach was intentional.

b. If employee misconduct was involved.

c. If the breach was a single incident or part of a broad-based criminal effort.

d. If the incident is part of an ongoing investigation by the Federal Bureau of Investigation (FBI), Secret Service, or other federal, state, or local law enforcem

e. If notice to individuals or third parties would compromise an ongoing law enforcement investigation.

Incidents involving potential employee involvement in breach incidents (i.e., employee misconduct) will be referred to the Office of the Inspector General (OIG) Special Investigations Division (SID), which is authorized to conduct employee misconduct investigations.

5. Program Manager of the Program Experiencing the Breach

   All HUD Program Offices shall develop and document procedures for reporting incidents in their System Security Plan (SSP) or similar documents. HUD Program Offices shall report incidents and participate on the Breach Notification Response Team to provide information and any required assistance to appropriately address and respond to the breach.

6. Assistant Secretary for Congressional and Intergovernmental Relations

   The Assistant Secretary for Congressional and Intergovernmental Relations shall develop and communicate breach information to Congress and respond to any Congressional inquiries.

7. General Deputy Assistant Secretary for Public Affairs

   The General Deputy Assistant Secretary for Public Affairs shall develop and communicate appropriate breach information to the public and address media inquiries.

8. Chief Procurement Officer

   The Chief Procurement Officer shall address credit monitoring acquisition requirements.

9. Departmental Privacy Act Officer

The Departmental Privacy Act Officer shall address all Privacy Act requirements.

10. Assistant Secretary of Administration

The Assistant Secretary of Administration shall provide senior management support, subject matter expertise and operational support in analyzing and responding to suspected or actual breaches that directly involve Departmental staff, physical security incidents, and identity management incidents.

11. Other

In addition, the Breach Notification Response Team will work closely with other Federal agencies, offices, and teams for ensuring that appropriate, risk-based, tailored responses to breaches are developed and implemented.

1-4 Incident Reporting Procedures

A. Pursuant to HUD Incident Reporting Procedures, all agency officials, staff, and contractors are directed to report immediately any suspected or known breach of nonpublic HUD information to the HUD National Help Desk at (888) 297-8689.

B. The following incident reporting procedures are established and shall be part of HUD's mandatory Security Awareness and Privacy Training program:

1. Upon notification of a breach, the HUD National Help Desk will then notify:

a. The HCSIRC in the event of the following events:

(1) Unauthorized Access

(2) Denial of Service

(3) Malicious Code

(4) Improper Usage

(5) Scans, Probes, and Attempted Access

b. The designated OCIO Office of Information Technology (IT) Operations manager point of contact at (202) 402-6160. In the

event the IT Operations manager cannot be contacted, the Help Desk will contact the HUD Computer Security Incident Response Center (HCSIRC) at 708-0614 extensions 3519, 3549, or 3560.

2. In the event that the incident falls under the category of unauthorized access, denial of service, or malicious code or involves PII,

   a. The IT Operations manager will notify:

      (1) HUD's CISO at (202) 401-8094 and

      (2) The HCSIRC during normal business hours at (202) 708-0614 extensions 3519, 3549, or 3560 and during off-hours at (304) 433-4381 or (202) 361-5764.

   b. The HCSIRC shall report the incident to the US-CERT.

   c. The HCSIRC shall track and manage each incident to completion.

   d. The Federal Information Security Management Act of 2002 requires all agencies to report security incidents to a Federal incident response center. The U.S. Computer Emergency Response Center (US-CERT), which is operated by the Department of Homeland Security, requires agencies to report incidents within various timeframes according to type of incident. OMB memorandum M-06-16, Protection of Sensitive Agency Information, now requires agencies to report all incidents involving PII to US-CERT within one hour of discovering the incident. Incidents to be reported may involve PII that is in either electronic or physical (hard copy) form and both suspected and confirmed breaches are to be reported.

1-5 Response to Breaches

A. Initiate Team. Within 24 hours of being notified of a breach, the CISO shall notify all members of the HUD Breach Notification Response Team. The CIO / Senior Official for Privacy shall, as appropriate, convene a meeting of the complete HUD Breach Notification Response Team or specific members, as needed.

B. Initial Assessment. The HUD Breach Notification Response Team shall evaluate the specific incident and situation to guide the development of an action and response plan. The HUD Breach Notification Response Team shall examine the data elements involved to determine the nature of the PII involved.

Determining what data have been compromised or potentially compromised is vital to making an accurate risk assessment and charting an appropriate course of action. As part of the initial evaluation, the following information shall be addressed:

1. Date of Incident

2. Person reporting the Incident

3. Person discovering the Incident

4. Nature of Incident and means by which the breach occurred, such as:

    a. Unauthorized access to information

    b. Unauthorized use of information

    c. Lost computer, storage device, or portable media

    d. System or network intrusion

    e. Loss of paper documents containing sensitive information

    f. Number of individuals potentially affected

    g. The information accessibility status

        (1) Unprotected

        (2) Encrypted

        (3) Rendered unusable

C. Investigation Responsibilities. If the HUD Breach Notification Response Team determines that the breach involved unintentional loss of control or disclosure of PII or Covered Information, the CIO shall have primary responsibility for the investigation. If an incident appears to involve the intentional disclosure of PII or Covered Information, the IG shall have primary responsibility for investigation. Incidents involving potential employee involvement in breach incidents (i.e., employee misconduct) will be referred to OIG 's Special Investigations Division (SID), which is authorized to conduct employee misconduct investigations.

D. Identify Theft

1. Risk Analysis. To determine if a breach is the basis for identify theft risk, the HUD Breach Notification Response Team shall evaluate the following factors, as identified in OMB M-07-16:

   a. Type of PII or Covered Information compromised.

   b. Ease or difficulty for an unauthorized person to access the information based on the protections established.

   c. Means by which the PII or Covered Information lose occurred, including where the incident might be the result of criminal activity or is likely the result of criminal activity.

   d. The ability of the Department to mitigate the identify theft.

   e. The evidence that substantiates that the comprised PII or Covered Information is being used to commit identity theft.

2. Response. If analysis determines that there is a risk of identity theft from a breach, the HUD Breach Notification Response Team shall develop a response plan to mitigate such risk. In developing this plan, the HUD Breach Notification Response Team shall consider the options available to agencies and individuals to protect potential victims of identity theft, as identified in OMB M-07-16:

   a. For individuals, options considered will include:

      (1) Contacting financial institutions.

      (2) Monitoring financial account activity.

      (3) Requesting a free credit report.

      (4) Placing fraud alert on credit reports.

      (5) For authorized state residents, placing a freeze on credit files.

      (6) For deployed military personnel, placing an active duty alert on credit file.

      (7) Information and resources provided at www.idtheft.gov.

b. The Department will also consider the following options:

(1) Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identify theft.

(2) Providing commercial credit monitoring services, adhering to the guidance provided in OMB M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements.

E. Risk of Harm Analysis. The HUD Breach Notification Response Team shall consider other likely risk of harm caused by the breach. These risks include harm to reputation or potential for harassment or prejudice, particularly when health or financial information is involved in the breach. The HUD Breach Notification Response Team shall consider the following five factors, as identified in OMB M-07-16:

1. Nature of the data elements breached and context of the data. The nature of the data elements compromised for each incident is a key factor to consider in determining when and how notification should be provided to affected individuals. For example, theft of a database containing individuals' names and Social Security Numbers (SSN) and/or dates of birth may pose a high level of risk, while a theft of a database containing only individuals' names may pose a low risk, depending on its context. The HUD Breach Notification Response Team shall consider the data element(s) and context involved and shall identify the potential harms and level of risk caused by the breach.

2. Number of individuals affected. The HUD Breach Notification Response Team shall consider the number of affected individuals when determining notification methods.

3. Likelihood the information is accessible and usable. The HUD Breach Notification Response Team shall assess the likelihood that PII or Covered Information will be or has been used by unauthorized individuals.

4. Likelihood the breach may lead to harm. The HUD Breach Notification Response Team shall 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 information which could result

in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

5. Ability of the agency to mitigate the risk of harm. The HUD Breach Notification Response Team shall assess the ability of the Department to mitigate or contain the breach.

F. Level of Impact. The HUD Breach Notification Response Team will assign a level of impact for the breach. The impact levels are:

1. Low. The loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

2. Moderate: The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

3. 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.

G. Notification

1. Notification of Individuals.

a. If the HUD Breach Notification Response Team, applying the criteria set forth in OMB M-07-16, determines that the likelihood exists that PII or Covered Information was acquired by an unauthorized person and that the information could be used for fraudulent purposes or could lead to harm, then the Incident Response Plan shall ensure that the affected individuals will be notified of the breach. This notice shall be provided without unreasonable delay but no later than 45 days after a determination is made.

b. The HUD Breach Notification Response Team shall consult with the IG or other law enforcement officials investigating the incident before making any public disclosures.

c. The HUD Breach Notification Response Team shall consider the following elements in the notification process:

(1) Timing. The Department shall provide notification of a breach without unreasonable delay, consistent with the

needs of law enforcement and national security. A decision to delay notification may be considered if immediate notification would seriously impede the investigation of the breach or the affected individual(s). However, no delay shall exacerbate risk or harm to any affected individual(s).

(2) Source of the notice. Notification of affected individual(s) shall be issued by the Secretary or by the Assistant Secretary of the impacted program. Notification for incidents involving only a limited number of individuals (e.g. under 50) may also be issued jointly under the auspices of the CIO / Senior Official for Privacy.

When the breach involves a Federal contractor or a public-private partnership operating a Departmental system of records on behalf the Department, the Department shall be responsible for issuing any breach notification and undertaking the appropriate corrective actions.

(3) Contents. All notifications shall be provided in writing and will be concise, conspicuous, and in plain language. Notices shall include:

- A brief description, including date(s) of the breach and of its discovery.
- Identification of the types of personal information involved.
- A statement that the information was encrypted or protected by other means, but only when this information would be beneficial and would not compromise the security of a system.
- Steps individuals should take to protect themselves from potential harm.
- Information on the steps the Department has underway to investigate the breach, to mitigate losses, and to protect against any further breaches.

- A point of contact for affected individuals to contact for more information, including a toll-free telephone number, e-mail address, and postal address.

(4) Method of notification. The notification methodology shall be commensurate with the number of individuals affected and the urgency with which notification is required. Possible methods of notification include telephone, first-class mail, e-mail, existing Government-wide services, newspapers or other public media outlets, or substitute notice. The Department shall ensure that the selected notice methodology is Section 508 compliant.

d. These elements shall be analyzed in accordance with guidance set forth in OMB M-07-16. In particular, the contents of any Departmental notice disseminated to individuals shall include the following:

(1) A brief description of what occurred.

(2) A description of the types of information involved.

(3) A brief description of what the Department is doing to investigate the breach, mitigate losses, and protect against further breaches.

(4) Identify point-of-contact information for individuals who have questions or need more information, including a toll-free number, TTY number, website, and/or postal address.

(5) Recommendations on actions that affected individuals can take in order to protect themselves from the risk of ID theft.

2. Notification to Third Parties

a. Notice to third parties shall be carefully coordinated with notice to individuals with regard to timing, order, and content of the notice. This coordination shall ensure that any ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate.

b. Based on the nature of the breach, notice to the following third parties may be considered:

(1) Law Enforcement. The HUD Breach Notification Response Team, the CISO, or the IG may notify federal, state, or local law enforcement.

(2) US-CERT. Incidents involving PII will report to the US-CERT within one hour or as soon as practical by the HUD Breach Notification Response Team.

(3) Media and the Public. The General Deputy Assistant Secretary for Public Affairs, in coordination with the HUD Breach Notification Response Team, is responsible for directing all meeting s and discussion with the news media and public. This includes the issuance of press releases and related materials on the Department's Internet website.

(4) Financial Institutions. If the breach involves government-authorized credit cards or individuals' bank account numbers that are used in employment-related transactions (e.g. payroll), the HUD Breach Notification Response Team will promptly notify the bank or other entity that is responsible for the particular transaction.

(5) Congress. The Assistant Secretary for Congressional and Intergovernmental Relations, in coordination with the HUD Breach Notification Response Team, is responsible for coordinating all communications and meetings with member of Congress and their staff. The HUD Breach Notification Response Team will notify the Assistant Secretary for Congressional and Intergovernmental Relations immediately when an issue arises that may require communications with member of Congress and their staff.

(6) Attorney General. The IG shall promptly notify the Attorney General of any criminal violations relating to the disclosure or use of PII and Covered Information, as required by the Inspector General Act of 1987, as amended.

1-6 Documentation

A. The HUD Breach Notification Response Team shall document each incident, action and response plan and actual responses. This information will be used for the purpose of tracking the management and disposition of specific

breaches. The HUD Breach Notification Response Team shall ensure that appropriate and adequate records are maintained to document breach responses reported under this plan.

B. In accordance with the Privacy Act of 1974 and the Federal Records Act, such records shall be generated, compiled, and maintained in manner sufficient to safeguard the financial, legal, or other rights of individuals, if any, affected by a breach, including any parallel law enforcement investigations, litigation, or other pending actions.

C. Incident documentation shall be maintained no longer than required by applicable records retention schedules to ensure that any sensitive PII and Covered Information in such records is not unnecessarily retained or exposed to a risk of breach. Such records shall be destroyed only in accordance with approved and secure methods designed to ensure against inadvertent disclosure, theft, or other compromise of personal or other nonpublic information.

1-7 Evaluation of Breach Response

A. The development and implementation of the HUD Breach Notification and Response Plan is an on-going process. As such, the management and disposition of all suspected or actual breaches will be evaluated by the HUD Breach Notification Response Team in an effort to identify more effect and efficient responses or identify tasks and make improvements or modifications as appropriate.