U.S. Department of Housing and Urban Development

Breach Notification Policy and Response Plan

Table of Contents

List of Figures

List of Tables

1. Introduction

This U.S. Department of Housing and Urban Development (HUD) *Breach Notification Policy and Response Plan* outlines HUD's approach for coordinating a response to a privacy incident. Additionally, this document complies with Office of Management and Budget (OMB) Memorandum 07-16, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information",* May 22, 2007, which requires all federal agencies to report privacy incidents, whether paper-, electronic-, or voice-based to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery/detection. In accordance with OMB's direction, HUD has developed this *Breach Notification Policy and Response Plan* to identify the most efficient and effective method of notification, in case of a breach, to the HUD Privacy Officer and other key designated officials. By aligning with current HUD guidance and addressing the unique organizational structure of HUD, the policy and plan ensure a comprehensive and cohesive response.

2. Scope

This document provides an outline defining policies and procedures in case of a privacy-related incident, whether paper-, electronic-, or voice-based. For purposes of this policy, a privacy-related incident is defined in terms of information about an individual owned or maintained by HUD, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and other information that can be used to distinguish or trace an individual's identity. "Other information" may be name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual[1]. This policy and plan apply to all HUD employees, HUD contractors, and HUD third parties, including Public Housing Authorities (PHA).

The concept of privacy is intrinsic to the nature of HUD's mission. Without HUD's strong adherence to federally required protection of personally identifiable information (PII), the public will not trust that HUD can maintain a customer's personal data that are required by the Federal housing programs. This will hinder HUD from providing services to those who need them most.

The following sections provide overviews both of privacy and PII and of the procedures that should take effect when there is a privacy incident. A separate document, the HUD privacy incident response standard operating procedures, provides additional information and detailed procedures that are to be enacted in the event of a privacy incident.

[1] OMB Memorandum 06-19, July 12, 2006 *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.*

3. Authorities

HUD is committed to safeguarding PII and implementing sound procedures for handling privacy incidents in accordance with numerous federal statutes, regulations, and directives, including the following:

- US Department of Housing and Urban Development Privacy Act Handbook 1325.01 REV-1;
- US Department of Housing and Urban Development Privacy Principles;
- OMB Circular A-130, which specifies that federal agencies will "ensure there is a capability to provide help to individuals when a security incident occurs in the system and to share information concerning common vulnerabilities and threats";
- The Federal Information Security Management Act of 2002 (FISMA), which directs that a program for detecting, reporting, and responding to security incidents be established in each department. FISMA also requires the establishment of a central federal information security incident center;
- OMB Memorandum 06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006, (M-06-15), which reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy;
- OMB's Memorandum entitled, *Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006, which outlines recommendations to agencies from the President's Identity Theft Task Force for developing agency planning and response procedures for addressing PII breaches that could result in identify theft;
- OMB Memorandum 06-16, *Protection of Sensitive Agency Information*, June 23, 2006 (M-06-16), which requires agencies to implement encryption protections for PII being transported and/or stored offsite;
- OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006 (M-06-19), which requires agencies to report all incidents involving PII to US-CERT within one hour of discovery of the incident;
- OMB Memorandum 09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, August 20, 2009 (M-09-29), which requires agencies to provide updated information on the agency's privacy management program (including incident response) as part of the FY2009 FISMA report to OMB;
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (M-07-16), which identifies existing procedures and establishes several new actions agencies should take to safeguard PII and to respond to privacy incidents;
- *Combating Identity Theft: A Strategic Plan*, April 23, 2007, drafted by the President's Identity Theft Task Force , which puts forth a comprehensive strategic plan for steps the

federal government can take to combat identity theft with recommended actions that can be taken by the public and private sectors. The report is available at www.idtheft.gov;

- The Privacy Act of 1974, 5 U.S. Code (U.S.C.) § 552a, which provides privacy protections for records containing information about individuals (i.e., citizen, legal permanent resident, and visitor) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records;
- The E-Government Act of 2002 (Public Law 107–347), which requires federal agencies to conduct Privacy Impact Assessments (PIA) for electronic information technology (IT) systems that collect, maintain, or disseminate PII and to make these assessments publicly available;
- Federal Information Processing Standard (FIPS) Pub 199, *Standards for Security Categorization of Federal Information and Information Systems,* February, 2004, which establishes standards to be used by all federal agencies to categorize all information collected or information systems maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels; and
- 5 Code of Federal Regulations (CFR) § 2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*, which establishes standards of ethical conduct for employees of the Executive Branch of the United States Government.

4. Definitions

4.1 Privacy

The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of PII about individuals that is maintained in systems of records (SOR) by federal agencies. A SOR is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their SORs by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a SOR absent the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to an amendment of their records and sets forth various agency record-keeping requirements.

4.2 Personally Identifiable Information

Personally Identifiable Information (PII) refers to information that can be used to distinguish or trace an individual's identity, such as name, social security number, and biometric records; individually or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[2]

[2] OMB M-07-16, May 22, 2007

Some examples of PII include name, date of birth (DOB), email address, mailing address, medical history, family relationships, vehicle identifiers including license plates, unique names, certificate, license, telephone and/or other specific reference numbers and/or any information that can directly identify an individual.

4.3 Sensitive Personally Identifiable Information

Sensitive Personally Identifiable Information (SPII) is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone data elements.

Some examples of SPII include biometric information (e.g., DNA, iris images, fingerprint, and photographic facial images), Social Security Number (SSN), account numbers, and any other unique identifying number (e.g., Federal Housing Administration [FHA] case number, driver's license number, or financial account number, etc.). Other data elements such as citizenship or immigration status; medical information; ethnic, religious, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.

4.4 Privacy Incident

A **privacy incident** is a violation or imminent threat of a violation of privacy laws, principles, policies, and practices. Breaches, which are situations where unauthorized individuals have access or potential access to PII, are one type of privacy incident.[3] However, there are other types of privacy incidents, including using PII for purposes other than the stated purpose for which the information was originally collected, exceeding the retention period for PII, and collecting and/or using PII without first providing proper notice. The term "privacy incident" encompasses both **suspected and confirmed incidents** involving PII and applies in either a classified or unclassified environment. It includes information in both electronic and paper format and information maintained in a system of records as defined by the Privacy Act.[4]

4.5 Computer Security Incident

A computer-security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[5]

4.6 HUD Computer Incident Response Team

The HUD Computer Incident Response Team (HUDCIRT) combats the disruptive short- and long-term effects of security threats, flaws, vulnerabilities, and incidents directed at HUD. The

[3] A breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized individuals and for any other than authorized purpose have access or potential access to[PII] in usable form, whether physical or electronic." OMB M-07-16

[4] OMB M-07-16

[5] NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004

maintains a security incident reporting and handling capability and is responsible for vulnerability scanning and monitoring and advising on operational and technical controls.

4.7 Harm

Loss or misuse of information adversely affects one or more individuals or undermines the integrity of a system or program. There is a wide range of harms, including anticipated threats or hazards to the security or integrity of records that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. The range also includes harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved**.**

To help with identifying the level of potential impact to individuals if there is a lack of privacy, it is useful to look at the types of potential harms that can result. The types of potential harms to individuals described below are due primarily to privacy violations, but can also be due to ambiguous identification, erroneous authentication, and/or inaccurate authorization. Types of harms are

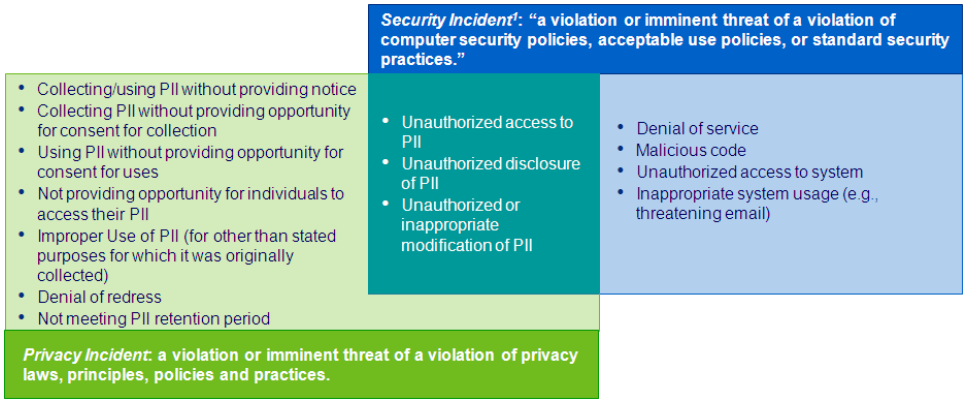
- **Social harms:** These include inconvenience, embarrassment, distress, increased vulnerability of the individual to social engineering or extortion, and/or damage to personal standing or reputation due to misuse, unauthorized disclosure, or inaccuracy of identifying or authorization-related information. Inconvenience can include the time and effort needed to cope with the misuse, to reduce the likelihood or mitigate the effects of identity theft (e.g., by closing and reopening accounts), or to make corrections. The type and extent of distress, embarrassment, vulnerability, or damage to personal standing or reputation depends on the nature and context of misuse (e.g., marketing use could produce pop-up ads for drugs, which could indicate possible medical conditions), the sensitivity of the disclosed information and on how broadly or to whom it was released, or the consequences of the information being inaccurate (e.g., being denied expected services in front of a valued client).
- **Physical harms:** These include distress due to misuse, unauthorized disclosure, or inaccuracy of identifying or authorization-related information. The type and extent of physical harm depends on the context of the misuse (e.g., profiling could lead to forcible detention), disclosure (e.g., information about an individual is made available to a stalker), or inaccuracy (e.g., an individual who is misidentified to a healthcare provider could receive incorrect medical treatment.) The level of harm depends in part on the potential for escalating damage if the individual disputes the identifying or authorization-related information.
- **Financial harms:** These harms typically involve financial loss or liability. Financial harms are often but not always due to identity theft. The consequences to the individual are highly dependent on how extensive the harm is and on what actions the thief takes if there is identity theft.

4.8 Security vs. Privacy Incidents

Not all security incidents are *privacy incidents* and, conversely, *not all privacy incidents* are *security incidents*, but some incidents can be both a *privacy incident* and a *security incident, as shown in the box in the center of Figure 4.9.* In this case, both the HUD Chief Information

Security Officer (CISO) and Privacy Officer must collaborate to develop the appropriate reporting artifacts.

Figure 4.9 - Security vs. Privacy Incidents



5. Privacy Incident-Handling Roles and Responsibilities

This section provides a description of the roles and responsibilities of the different individuals and groups who play a major role in the privacy incident-handling process at HUD.

5.1 HUD Breach Notification Response Team

The HUD Breach Notification Response Team (HBNRT) is a core group of HUD privacy stakeholders responsible for managing a privacy incident lifecycle, including preparation, detection and risk analysis, triage and escalation, response and recovery, and coordination of any post-incident activities with the HUDCIRT.

In collaboration with the Privacy Officer, the HBNRT is responsible for involving other key stakeholders to assist with the appropriate follow-up after a privacy incident and for escalating and/or notifying an incident alert and involving other entities within HUD and other key officials within stakeholder organizations (as necessary).

5.1.1 General Responsibilities of Each Member

- Provide advice, expertise, and assistance to the entire HBNRT, where necessary, and handle privacy incidents in consultation with other members of the team.
- Provide recommendations and assistance to the Chief Information Officer (CIO) regarding the investigation, notification, and mitigation of High-Impact and Moderate-Impact privacy incidents.
- Coordinate with external entities such as law enforcement during the investigation, notification, or mitigation stages of High-Impact or Moderate-Impact privacy incidents as warranted.
- Review implementation of this guidance at least annually or whenever there is a material change in HUD practices.

5.1.2 Specific Roles and Responsibilities

Specific roles and responsibilities for members of the HBNRT are provided below.

5.1.2.1 Senior Agency Official for Privacy (SAOP)

- Chair the HBNRT.
- Convene the HBNRT as needed.

5.1.2.2 Privacy Officer

- Work in close consultation with the CISO and IT Security regarding privacy-incident handling and other privacy issues affecting IT systems.
- Work with the CISO and IT Security to ensure a complete and accurate Privacy Incident Report.
- Consult with the CIO, Deputy CIO, Associate CIO for Information Assurance, and CISO concerning privacy incident handling.
- Work with the CISO and IT Security to contain privacy incidents.
- Work with the CISO and IT Security to assess the likely risk of harm posed by the privacy incident (e.g., Low-, Moderate-, or High- impact) to determine who should handle the investigation, notification, and mitigation of the incident.
- Handle the investigation, notification, and mitigation for privacy incidents working with the CISO and IT Security.
- Draft documents as warranted by the privacy incident-handling process working with the CISO.
- Make joint decisions with the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release in Low- and Moderate-Impact privacy incidents that occurred and provide recommendations to the CIO.
- Provide internal notification to HUD senior officials prior to the authorized public release of information related to privacy incidents.
- Make incident-closure recommendations in consultation with the HBNRT.
- Maintain and update point-of-contact (POC) information for privacy incident handling.
- Prepare an annual report for the CIO outlining the lessons learned from privacy incidents that occurred during the year and identifying ways to strengthen Departmental safeguards for PII and to improve privacy-incident handling.
- Brief the CIO and senior management on the status and outcome of ongoing and completed privacy incidents.

5.1.2.3 Chief Information Security Officer

- Work in close consultation with the Privacy Officer regarding privacy incident handling and other privacy issues affecting information technology systems.
- Work with the Privacy Officer to ensure a complete and accurate privacy incident Report.
- Consult with the CIO, Deputy CIO, Associate CIO for Information Assurance, and Privacy Officer concerning privacy-incident handling.
- Work with the Privacy Officer to contain privacy incidents.

- Work with the Privacy Officer to assess the likely risk of harm posed by the privacy incident (e.g., low, moderate, or high impact) to determine who should handle the investigation, notification, and mitigation of the incident.
- Handle the investigation, notification, and mitigation for privacy incidents working with the Privacy Officer.
- Draft documents as warranted by the Privacy Incident Handling Process working with the Privacy Officer.
- Make joint decisions with the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release in Low- and Moderate-Impact privacy incidents that occurred and provide recommendations to the CIO.
- Make incident closure recommendations in consultation with the HBNRT.
- Examine monthly reports issued by US-CERT addressing the privacy incidents that were reported to US-CERT.

5.1.2.4 Other Members

5.1.2.4.1 Assistant Secretary for Congressional and Intergovernmental Relations

- Consult and coordinate with the CISO and Privacy Officer to determine when notification of the Congressional Oversight Committee Chair is necessary for a privacy incident.
- Respond to Congressional inquiries related to privacy incidents.

5.1.2.4.2 Associate Chief Information Officer for Information Assurance

- Advise the CIO and the Deputy CIO on all matters pertaining to privacy and the privacy/security interface.
- Consult with the CIO, Deputy CIO, CISO, and Privacy Officer concerning privacy-incident handling.

5.1.2.4.3 Chief Financial Officer

- Serve as a member of the HBNRT when Chief Financial Officer (CFO)-designated financial systems are involved in the privacy incident.
- Approve reimbursement of expenses related to investigation of privacy incidents.
- Notify the issuing bank when the privacy incident involves government-authorized credit cards.
- Notify the bank or other entity involved when the privacy incident involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government salaries, travel vouchers, or any benefit payment.
- Provide recommendations to the Chair of the HBNRT and the Component Head in consultation with other members of HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release in privacy incidents involving CFO-designated financial systems.

5.1.2.4.4 Chief Information Officer

- Act as SAOP.

- Provide management direction to security operations.
- Serve as an advocate for privacy and computer security incident response activities in consultation with the CISO and Privacy Officer.
- Advise the Secretary of any issues arising from privacy incidents that affect infrastructure protection, vulnerabilities, or issues that may cause public concern or loss of credibility.
- Ensure that incidents are reported within the required reporting time requirements.
- Provide recommendations to the Secretary in consultation with the CISO, Privacy Officer, and other members of the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Advise the Secretary on the applicability of privacy incidents for communication to the White House.

5.1.2.4.5 Chief Procurement Officer

- Address credit monitoring acquisition requirements when it is determined that credit monitoring will be offered.

5.1.2.4.6 Customer Relationship Manager

- Provide recommendations to the HBNRT regarding managing interactions with external entities who engage with HUD and may potentially be affected by privacy incidents.

5.1.2.4.7 General Counsel

- Provide legal advice to the HBNRT regarding the potential for disciplinary action or corrective action against HUD personnel arising from a privacy incident.
- Provide recommendations to the CISO and Privacy Officer in consultation with other members of the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Provide advice on whether referral of a privacy incident to other authorities is warranted.
- Serve 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.
- Review, revise, and comment on reports and corrective actions taken.

5.1.2.4.8 General Deputy Assistant Secretary for Public Affairs

- Work with the HBNRT to coordinate the external notification to affected third parties and the issuance of a press release.
- Serve as sole point-of-contact for media-related inquiries about privacy incidents.

5.1.2.4.9 Human Capital Officer

- Work with the CFO, Privacy Officer, or other members of the HBNRT as needed in privacy incidents involving individuals' bank account numbers to be used for the direct deposit of credit-card reimbursements, government employee's salaries, or any benefit information.
- Consult with the Secretary or designee(s) in cases involving potential disciplinary or corrective action arising from a privacy incident.

- Maintain a record of all disciplinary or corrective actions taken against HUD personnel that arise out of a privacy incident.

5.1.2.4.10 Inspector General

- Consult with the CISO and Privacy Officer on a case-by-case basis to determine the appropriate incident handling procedures for Moderate- and High-Impact privacy incidents as warranted.
- Provide recommendations to the CISO and Privacy Officer in consultation with other members of the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Conduct an investigation to determine
  - If the breach was intentional.
  - If employee misconduct was involved.
  - If the breach was a single incident or part of a broad-based criminal effort.
  - If the incident is part of an ongoing investigation by the Federal Bureau of Investigation, Secret Service, or other federal, state, or local law enforcement.
  - 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 (IG) Special Investigations Division, which is authorized to conduct employee misconduct investigations.
- 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.

5.1.2.4.11 Program Manager of the Program Experiencing the Breach

- Ensure compliance with federal laws and Departmental privacy policy concerning the operation and maintenance of information systems and programs.
- Recognize privacy incidents.
- Understand the privacy incident-reporting process and procedures.
- Understand how to contact the HUD Help Desk when a privacy incident occurs.
- Receive initial reports from HUD personnel regarding the possible detection of privacy incidents.
- Consult with the Privacy Officer when necessary to obtain guidance concerning privacy incident handling and other privacy issues affecting information systems.
- Determine whether a suspected or confirmed incident involving PII may have occurred.
- Assist the CISO and Privacy Officer with the development of facts for the Privacy Incident Report.
- Assist with the investigation and mitigation of a privacy incident to the extent necessary.

5.1.2.4.12 Senior Advisor to the Secretary

- Provide recommendations to the Secretary in consultation with members of the HBNRT regarding the handling of privacy incidents.

5.2 Other Individuals and Entities

General privacy incident-handling responsibilities for individuals and entities who are not members of the HBNRT are provided below.

5.2.1 Deputy Secretary

- Consult with HUD senior officials regarding the handling of privacy incidents as warranted by the circumstances.
- Provide recommendations to the Secretary in consultation with members of the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release.

5.2.2 Chief Operating Officer

- Provide recommendations to the HBNRT regarding the impact upon HUD operations of privacy incidents and potential approaches for handling incidents.

5.2.3 Deputy Chief Information Officer

- Act as Chair of the HBNRT in the SAOP's absence.
- Receive immediate notification of privacy incidents reported to the US-CERT.
- Advise the CIO on the applicability of privacy incidents for communication to the White House.

5.2.4 HUD Computer Incident Response Team

- Notify the US-CERT when a reported incident involves PII.

5.2.5 HUD Help Desk

- Act as the First Responder for privacy incidents by processing reports of suspected or confirmed incidents involving PII.
- Recognize privacy incidents.
- Understand the privacy incident reporting process and procedures.
- Create a Help Desk Service Ticket and initial Privacy Incident Report and notify the HUD IT Operations (Ops) Manager.

5.2.6 HUD Personnel

- Attend periodic Privacy Awareness Training and Education.
- Recognize privacy incidents.
- Upon the detection or discovery of suspected or confirmed incidents involving PII, contact the Program Manager or other "responsible official," such as a supervisor.

5.2.7 IT Operations Manager

- Notify the CISO and Privacy Officer when a reported incident involves PII.
- In the absence of the Privacy Officer, notify the HUDCIRT.

5.2.8 HUD Employees and Third Parties

- Maintain the privacy and security of all PII.
- Use PII only for the purposes intended.
- Follow all HUD procedures for the use, dissemination, and storage of PII.

6. Privacy Incident Impacts

6.1 Privacy Incident Impact Levels

The three levels of impact of privacy incidents range from the least severe (Privacy Incident Impact Level 3) to most severe (Privacy Incident Impact Level 1), depending on the sensitivity of PII; the number of individuals whose PII is involved; and the harm that may result or has resulted from the illegal, unauthorized, unethical disclosure, modification, use or disposal of the information. For purposes of incident handling, all incidents involving sensitive PII are categorized as High.

- Privacy Incident Impact Level 3, Low-Impact
- Privacy Incident Impact Level 2, Moderate-Impact
- Privacy Incident Impact Level 1, High-Impact

Levels of a privacy incident based on the potential impact are described below.

Table 6.1 – Impact Levels of a Privacy Incident

Level/Impact	Definition
3 – Low	The unauthorized, unethical disclosure, use or disposal of information that could cause a **limited adverse effect** on organizational operations or on affected individuals.
2 – Moderate	The illegal, unauthorized, unethical disclosure, modification, use or disposal of information that could cause an **adverse effect** on organizational operations, assets, and/or on affected individuals.
1 – High	The illegal, unauthorized, unethical disclosure, modification, use or disposal of information that could cause **a serious adverse effect** on organizational operations, assets, reputation, and affected individuals.

Guidelines for determining appropriate privacy incident impact level:

Table 6.2 - Privacy Incident Impact Level

Privacy Incident Impact Level	Definition
Privacy Incident Impact Level 3 (Low)	No SPII involved Low impact (distress, inconvenience or corrective action) to affected individuals Minimal corrective action required by HUD
Privacy Incident Impact Level 2 (Moderate)	No SPII involved Moderate impact (distress, inconvenience, or corrective action) to affected individuals Significant corrective action possibly required by HUD
Privacy Incident Impact Level 1 (High)	SPII involved Potentially high impact (distress, inconvenience or corrective action) by affected individual(s) Potentially adverse effect on organizational operations, assets, reputation, and affected individuals

Examples of appropriate incident categorization:

Table 6.3 - Privacy Incident Examples

Privacy Incident Category	Examples
Privacy Incident Impact Level 3 (Low)	A Compact Disk (CD) with a summary report of 15 individuals appears to be lost in an intra-office move. A HUD employee/contractor is caught browsing personal information of individuals for no apparent official purpose.
Privacy Incident Impact Level 2 (Moderate)	A laptop containing passport information of 30 individuals is lost. An envelope with 200 names and mailing addresses of individuals with redress inquiries is missing.
Privacy Incident Impact Level 1 (High)	A file with detailed information depicting the income levels of housing recipients, including name, SSN, date of birth (DOB) and address is lost in a public train station. Identifying information of 50,000 individuals is exposed on-line for several hours after a computer breach by an unknown hacker.

6.2 Illustrations of Privacy Incidents

The following are some examples of privacy incidents. These examples are not exhaustive and are intended for illustration purposes only.

6.2.1 Loss of Control

- An employee reports that he cannot find a lost thumb drive that was ***not encrypted or password protected*** containing ***the names, telephone numbers, and badge numbers of contractors.*** The employee believes the thumb drive is somewhere in the building.
- A supervisor reports that hotel security officers recovered an encrypted/password-protected personal laptop that was temporarily stolen for two days. Information contained in the laptop included ***employee/contractor names, identification (ID) numbers, grade and salary information, home addresses, and home telephone numbers***.

6.2.2 Compromise

- A broken lock is discovered on a cabinet that safeguarded ***sensitive financial records and account numbers***. The lock shows obvious signs of being forcibly broken.

6.2.3 Unauthorized Disclosure

- A copy of a ***completed Standard Form (SF)-86, which lists an SSN and personal financial information,*** was shared with a lawyer for use in a divorce proceeding without the subject's permission.
- Security clearance documents containing the sensitive ***PII*** of employees were faxed in error to the wrong agency's security office.

6.2.4 Unauthorized Acquisition

- An employee uses another employee's password and pin to copy government credit-card numbers and Personal Identification Numbers.
- A visitor takes a file containing the names, credit reports, authorization files, and signatures of employees that she finds in a conference room.

6.2.5 Unauthorized Access (Internal and External)

- A contractor misuses administrator privileges to view sensitive information on ***contract bids, government procurement-card numbers, and tax identification numbers.***

7. HUD Privacy Incident-Reporting Process

Upon discovery of a suspected or verified privacy incident, HUD personnel will immediately inform their Program Manager. If the Program Manager is not available, HUD personnel will inform another responsible official, such as a supervisor, of the incident. The Program Manager or other responsible official will alert the HUD Help Desk, which will then open a problem ticket and fill out the HUD Breach Incident Report Form. If a responsible official is informed of the incident first, then he or she must also notify the Program Manager of the incident.

The Help Desk will notify the HUDCIRT and provide a service desk ticket number and information obtained in the incident report. If the Help Desk is not available, the Program Manager or other responsible official will notify the HUD IT Operations Manager, who will contact the HUDCIRT.

The HUDCIRT will verify the incident and will then notify the CISO, the HUD Privacy Officer, US-CERT, and the IT Operations Manager (if the Operations Manager has not initiated the contact).

Upon notification by HUDCIRT, the CISO notifies the Deputy CIO. In the CISO's absence, either the Privacy Officer or the Security Office staff will contact the Deputy CIO.

The HUD CISO and Privacy Officer will review the incident and convene the HBNRT, when appropriate. The HBNRT will conduct a risk analysis to determine the extent of the incident. Depending upon the severity, the HBNRT will contact Law Enforcement, the IG and other agencies and entities as required. The CISO and the Privacy Officer will update the DCIO with the results of the analysis.

HUD must notify US-CERT within one hour of discovery/detection of a breach, regardless of the time required for processing the incident by HUD.

7.1 Report Content

Reports shall include a description of the incident or event and as much of the information listed below as possible; however, reporting should not be delayed in order to gain additional information:

- Incident category type—privacy incidents are always Privacy CAT 1 Incidents (Unauthorized Access or Any Incident Involving Personally Identifiable Information) for purposes of US-CERT categorization and will be prioritized based on the nature and severity of the incident.
- Point of contact information of person reporting incident (name, telephone, email and physical location (Office or Space Number)).
- Date and time of incident, and brief description of the circumstances surrounding the potential loss of PII, including
  - Summary of the type of information that is potentially at risk (e.g., explain that an individual's full name, SSN, birth date, etc., may have been compromised, but do not disclose specific PII in the report) (refer to the definitions of PII above for additional examples).
  - System name.
  - Location of the system(s) involved in the incident (Washington DC, Los Angeles, CA).
  - The Program Office in which the incident occurred.
  - Name, phone number, and email address of the person who discovered the incident.
- Interconnectivity of the system to other systems.
- Whether the incident is either suspected or confirmed.

- How PII was disclosed (e.g., email attachment, hard copy, stolen or misplaced laptop, etc.).
- To whom it was disclosed.
- Whether it was disclosed internally, within HUD.
- Whether it was disclosed externally.
  - If external disclosure is involved, state whether it was disclosed to the federal government, public, state/local government, foreign governments, and or commercial entities.
- Risk of the PII's being misused, expressed in terms of impact and likelihood.
- Security controls used to protect the information (e.g., password-protected, encryption (WinZip with AES encryption).
- Steps that have already been taken to reduce the risk of harm.Any additional steps that may be taken to mitigate the situation (e.g., base credit report, credit monitoring, appropriate destruction of electronic and hard copies).

7.2 HUD Computer Incident Response Team

The HUDCIRT is available to all program areas that need assistance in cyber security and privacy incident handling and gathering of incident information. In reporting cyber-related and privacy incidents to the HUDCIRT, provide as much detailed information as possible about how the incident occurred, what occurred, its impact, and what preventive measures have been implemented. Supply any log file information from the compromised system(s), routers, and/or firewalls in the communication path. HUDCIRT will analyze this information and provide recommendations to remediate the problem.

An incident involving the loss or suspected loss of PII must be reported to the US-CERT within one hour of HUDCIRT being notified of such an incident's occurring. The Privacy Officer and the CISO will also be notified of the loss or suspected loss of PII in accordance with HUDCIRT's Security Deliverables Distribution spreadsheet (located on the website: http://hudsharepoint.hud.gov/sites/main/OCIO/ITO/ivv/default.aspx.)

Incidents that will always be reported as involving the loss or suspected loss of PII are identified in Section 2.6, "Incident Handling Guidance for Selected Incidents", in the HUD Computer Incident Response Team Concept of Operations (version 1.7 rel. 10/26/09 or version in effect at the time).

HUDCIRT understands that this information is not always readily available; however, any details provided will help with the analysis. Even if an incident is resolved without the help of HUDCIRT, the incident should be reported. Incident analysis is valuable to HUD in comparing this incident with those reported by other sites. It further assists HUDCIRT in analyzing the HUD corporate threat and providing HUD, Privacy Officer and the CISO with guidance. In assessing the significance and reporting of such cyber security and privacy incidents, the reporting organization must consider the following questions and seek answers:

7.2.1 How?

- How was access gained?

- How was the incident detected?

7.2.2 What?

- What type of information was compromised (e.g., public, personal, or financial)?
- For information technology-related incidents:
  - What vulnerability was exploited?
  - What service did the system provide (Domain Name System [DNS], key asset servers, firewall, Virtual Private Network [VPN] gateways, Intrusion Detection System [IDS])?
  - What level of access did the intruder gain?
  - What hacking tools and/or techniques were used?
  - What did the intruder delete, modify, or steal?
  - What unauthorized data collection programs, such as sniffers, were installed?
  - What was the impact of the attack?
  - What preventative measures have been (are being) implemented?

7.2.3 Who?

- Determine responsible party's identification. These are usually Internet Protocol (IP) address (es) or host name(s) for IT-related incidents.

7.2.4 When?

- When was the incident detected?
- When did the incident actually occur?

8. Notification Process

8.1 Is Notification Required?

To determine whether notification of a breach is required, first assess the likely risk of harm caused by the breach and then assess the level of risk. Five factors should be considered to assess the likely risk of harm. Additional information on these factors is provided in OMB M-07-16.

- *Nature of data elements breached.* Consider data elements in light of their context and potential harm from disclosure. This is the key factor in determining whether notification is needed. Remember that compromised data may be low risk. However, when combined with other information, it could become high risk.
- *Number of individuals affected.* Should be considered when deciding how to notify the individuals, but should not alone be a determining factor whether to provide notification.
- *Likelihood the information is accessible and usable.* Consider how the information was protected (e.g., encryption, password) to determine how likely it is that the information will be used by unauthorized individuals.
- *Likelihood the breach may lead to harm.* Two factors to consider are

- Likelihood harm will occur. Consider the likelihood that an unauthorized individual knows the value of the information and will either use the information or sell it to others.
- Broad reach of potential harm. Consider potential for breach of confidentiality or fiduciary responsibility, for blackmail, for disclosure of private facts, for secondary uses of the information, or unwarranted exposure leading to humiliation or loss of self-esteem.
- *Ability to Mitigate the Risk of Harm.* Consider how the risk of harm can be mitigated to avoid further compromise of the data. While the ability to mitigate risk is not a key factor in determining whether to provide notification, it should be considered when deciding on timing of notification. Measures taken to mitigate risk should be put in place and should be mentioned in the notification unless it compromises an active investigation of the activities related to the breach.

8.2 Notification of Individuals

If the HBNRT, applying the criteria set forth in OMB M-07-16, determines that the likelihood exists that 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 HBNRT 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.

The HBNRT shall consult with the IG or other law enforcement officials investigating the incident before making any public disclosures.

The HBNRT shall consider the following elements in the notification process:

- *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).
- *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 Department SOR on behalf of the Department, the Department shall be responsible for issuing any breach notification and undertaking the appropriate corrective actions.
- *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 PII and related 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 POC for affected individuals to contact for more information, including a toll-free telephone number, e-mail address, and postal address.
- *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.

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:

- A brief description of what occurred.
- A description of the types of information involved.
- A brief description of what the Department is doing to investigate the breach, mitigate losses, and protect against further breaches.
- 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.
- Recommendations on actions that affected individuals can take in order to protect themselves from the risk of identity theft.

8.3 Notification of Third Parties

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.

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

- *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.
- *Congress*. The Assistant Secretary for Congressional and Intergovernmental Relations, in coordination with the HBNRT, is responsible for coordinating all communications and meetings with members of Congress and their staff. The HBNRT will notify the Assistant Secretary for Congressional and Intergovernmental Relations immediately when an issue arises that may require communications with members of Congress and their staff.
- *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 HBNRT will promptly notify the bank or other entity that is responsible for the particular transaction.
- *Law Enforcement*. The HBNRT, the CISO, the Privacy Officer, or the IG may notify federal, state, or local law enforcement.

- *Media and the Public*. The General Deputy Assistant Secretary for Public Affairs, in coordination with the HBNRT, is responsible for directing all meetings and discussion with the news media and public. This coordination includes the issuance of press releases and related materials on the Department's Internet website.

9. Acronyms

CD	Compact Disk
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DNS	Domain Name System
DOB	Date of Birth
FHA	Federal Housing Administration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HBNRT	HUD Breach Notification Response Team
HUDCIRT	HUD Computer Incident Response Team
HUD	United States Department of Housing and Urban Development
IDS	Intrusion Detection System
IG	Inspector General
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
Ops	Operations
PHA	Public Housing Authority
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

POC	Point of Contact
SAOP	Senior Agency Official for Privacy
SOR	System of Record
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network