U.S. Department of Housing and Urban Development

HUD Breach Notification Response Team (HBNRT)

Privacy Breach Standard Operating Procedures

Table of Contents

List of Figures

List of Tables

1. Overview

The U.S. Department of Housing and Urban Development (HUD) Breach Notification Policy and Response Plan (HBNRP) 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.

The concept of Privacy is intrinsic to the nature of HUD's mission. Without strong adherence to federally required protection of personally identifiable information, the public will not trust that HUD can maintain the sensitive customer personal data required by federal affordable housing programs. Loss of trust could impede HUD's ability to provide services to those who need them most.

HUD is committed to the privacy of its customers and expects compliance with these SOPs to maintain and increase public trust.

2. Scope

This document provides Standard Operating Procedures for the HUD Breach Notification Response Team (HBNRT) for handling and managing Privacy-related incidents, whether paper-, electronic-, or voice-based. The standards established in this document derive from various US Laws, Federal Mandates, Presidential Directives, Federal Guidance, accepted industry standards and best practices.

The portion of this Standard Operating Procedure pertaining to incident detection and reporting applies to all HUD employees, HUD contractors, and HUD third parties, including Public Housing Authorities (PHAs).

The following sections provide overviews both of privacy and personally identifiable information and of the procedures that occur when there is a privacy incident.

3. Definitions

3.1 Privacy

The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information 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.

3.2 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.[1]

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.

3.3 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 numbers (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.

3.4 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. 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.

3.5 Breach

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."[2]

[1] OMB M-07-16, May 22, 2007.

[2] Privacy Act of 1974.

3.6 Notice

Privacy safeguards that are required in the Privacy Act in Section (b) include permitting an individual to 1.) determine what records pertaining to him or her are collected, maintained, used, or disseminated by agencies; 2.) prevent records pertaining to an individual obtained by agencies for a particular purpose from being used or made available for another purpose without the individual's consent, and 3.) gain access to information pertaining to himself or herself in agency records. One of the mechanisms that is used to meet the above requirements is to provide notice, which is essentially a description of an organization's privacy protection practices. The Privacy Act specifically requires notice through the requirement to publish a description of the character of a system of records, known as a System of Records Notice (SORN), in the Federal Register whenever a system of records is established or revised (see Section (e) (4) of the Privacy Act). The Privacy Act also requires notice through its requirement for agencies to provide Privacy Act Statements to individuals whom the agencies are asking to supply information about themselves (see Section (e) (3) of the Privacy Act).

3.7 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.[3]

3.8 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

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

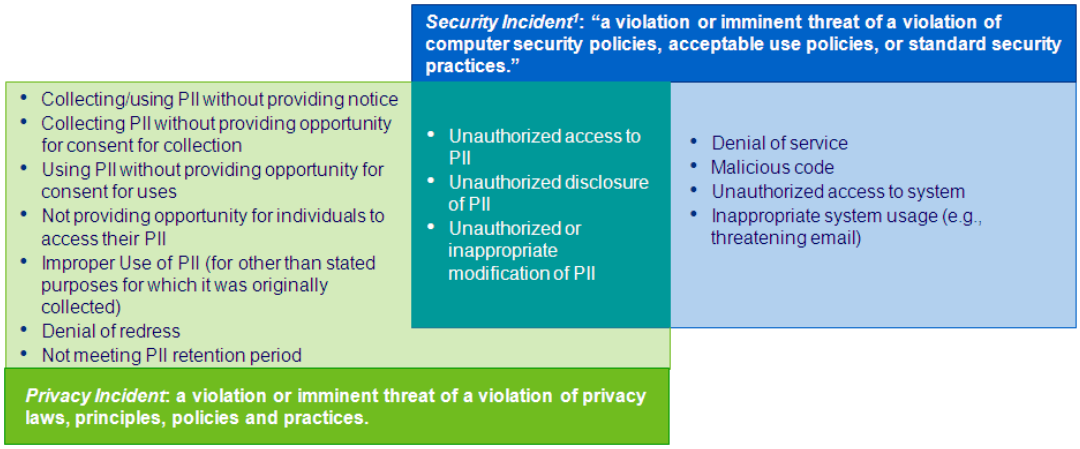
of the information being inaccurate (e.g., being denied expected services in front of a valued client).

- **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.

3.9 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 3-1*. In this case, both the HUD Chief Information Security Officer (CISO) and Privacy Officer must collaborate to develop the appropriate reporting artifacts.

Figure 3-1: Security vs. Privacy Incidents



4. 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.

4.1 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).

4.2 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.

4.2.1 Specific Roles and Responsibilities

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

4.2.1.1 Senior Agency Official for Privacy (SAOP)

- Chair the HBNRT.
- Convene the HBNRT as needed.
- Review and approve all HBNRT meeting minutes and notes.

4.2.1.2 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.

4.2.1.3 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.

4.2.1.4 Other Members

4.2.1.4.1 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.

4.2.1.4.2 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.

4.2.1.4.3 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.

4.2.1.4.4 Chief Information Officer

- 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.

4.2.1.4.5 Chief Procurement Officer

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

4.2.1.4.6 Customer Relationship Manager

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

4.2.1.4.7 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.

4.2.1.4.8 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.

4.2.1.4.9 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.

4.2.1.4.10 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.

4.2.1.4.11 Affected Program Manager

- 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 National 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.

4.2.1.4.12 Senior Advisor to the Secretary

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

4.3 Other Individuals and Entities

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

4.3.1 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.

4.3.2 Chief Operating Officer

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

4.3.3 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.

4.3.4 HUD Computer Incident Response Team (HUDCIRT)

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

4.3.5 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.

4.3.6 HUD Personnel

- Attend periodic Privacy Awareness Training and Education.
- Maintain the privacy and security of all PII.
- 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.
- Use PII only for the purposes intended.
- Follow all HUD procedures for the use, dissemination, and storage of PII. Recognize privacy incidents.

4.3.7 Associate CIO for Service Delivery

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

4.3.8 HUD 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. Recognize privacy incidents.

5. Privacy Incident Response Process

5.1 Incident Detection and Reporting

The privacy incident response process activates upon the discovery and report of a privacy incident. All HUD employees, HUD contractors, and HUD third parties must report a privacy incident regardless of whether the PII is in electronic, including voice, or physical form.

- 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. If a responsible office is informed of the incident first, then he or she must also notify the Program Manager of the incident.
- The Program Manager or other responsible official alerts the HUD Help Desk (1-888-297-8689 – Select option 9 for assistance).
- The HUD Help Desk opens a trouble ticket (in ServiceDesk) and collects information about the incident
- The HUD Help Desk will verify the incident by filling out the HUD Breach Incident Response Form with all information available at the time. The Breach Incident Response Form should contain as much of the information described within Section 5.1.2 as possible, if applicable, and to the extent the information is immediately available; however, reporting should not be delayed in order to gain additional information.
- Once it is determined that the trouble ticket involves a privacy incident, the HUD Help Desk transfers the ticket to HUDCIRT, and provides a copy of the HUD Breach Incident Report Form.
- If the Help Desk is not available, the Program Manager or other responsible official will notify the HUD IT Operations Manager, who will fill out the HUD Breach Incident Report Form and contact the HUDCIRT in placement of HITS.
- HUDCIRT reviews the ticket.
- HUDCIRT notifies the CISO and/or Privacy Officer of the event.
- The CISO will notify the Deputy CIO and the appropriate Associate CIO of the event. In the CISO's absence either the Privacy Officer or the Security Office Staff will notify the Deputy CIO.
- The HUDCIRT reports the event to the US-CERT within one hour of receiving the ticket.
- HUDCIRT tracks, monitors progress, and conducts some forensic investigation if the incident involves technology related losses.
- HUDCIRT operating procedures are available from: http://hudsharepoint.hud.gov/sites/main/OCIO/ITO/ivv/default.aspx.).
- HUDCIRT will analyze the HUD corporate threat and provide HUD, Privacy Officer and the CISO with guidance.

5.2 Report Content

The Breach Incident Report 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).
- 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).

6. Preliminary Investigation, Risk Analysis and Escalation

6.1 Preliminary Investigation

A preliminary investigation will enable HUD to tailor its response to a Privacy Incident based upon the severity of the incident and help identify the proper personnel required to handle the incident.

The CISO and PO will initiate the first phase in responding to a privacy incident by examining the information available to determine:

- The incident is real – there has been a violation of any Privacy laws, privacy policies and/or unauthorized access or loss of control of PII (see section 7.1.1).
- Determine initial privacy impact –. Complete the initial privacy risk management worksheet (see section 6.1.4).
- The privacy-level impact is based on the following information:
  - The nature of the data elements involved
  - The likelihood of that PII is accessible and usable

  - The likelihood that the privacy incident may lead to harm
  - The ability to mitigate the risk of harm
- The approximate number of individuals affected.
- Preliminarily, whether notification is warranted

Additional information may be necessary to validate the preliminary risk analysis and Impact Level decision. Additional information includes

- How was access gained?
- How was the incident detected?
- When was the incident detected?
- When did the incident actually occur?
- The type of information was compromised (e.g., public, personal, or financial)?
- What preventative measures have been (are being) implemented?
- Was the incident inside a trusted Departmental site?
- 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?
  - Were specific systems targeted, where are they located physically and on the network?
  - Is the incident inside the trusted network
  - Determine responsible party's identification. These are usually Internet Protocol (IP) address(es) or host name(s) for IT-related incidents.

6.2 Identity Theft Assessment

The Privacy Officer/CISO evaluates whether the data elements constitute the type of information that may pose a risk of identity theft (e.g., types include: (1) SSN; or (2) name, address, or telephone number combined with: (a) any government-issued identification number; (b) biometric record; (c) financial account number together with a PIN or security code (if a PIN or security code is necessary to access the account); or (d) any additional specific factor that adds to the personally identifying profile of a specific individual; (3) date of birth, password, and mother’s maiden name); or (4) Sensitive PII, such as SSN, driver's license number; financial account number; citizenship or immigration status; or medical information.

- If the Privacy Officer/CISO neither suspects nor confirms that identity theft is implicated, then the Privacy Officer/CISO proceeds with the investigation.
- If identity theft is implicated, the Privacy Officer/CISO immediately notifies the HUD Office of the Inspector General (OIG). Together, in close consultation, they analyze and complete the investigation.

6.3 If the Impact Level is Determined to be Impact Level 3 (Low):

The PO and CISO manage the incident using normal incident response procedures. They work with appropriate personnel including program office personnel, IT Operations personnel, HUDCIRT, the Office of General Counsel and the Inspector General.

1. Gather incident data
2. Conduct Analysis and Assessment
3. Work with the program area experiencing the incident:
   - To determine how to quickly contain the incident
   - To develop a response strategy
   - How quickly the strategy can be implemented
4. Ensure documentation of the incident is updated
5. Take steps to prevent any further incidents

Continue to Mitigation Section to review steps.

Privacy Officer provides monthly reports on Impact Level 3 incidents to the SAOP and OCIO management team.

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

6.4 If the Impact Level is determined to be Impact Level 2 (Moderate)

The Privacy Officer and CISO review the incident with the SAOP, and the SAOP determines whether to convene the HBNRT. If the HBNRT is not convened, the Privacy Officer and CISO manage the incident using normal incident response procedures. They work with appropriate personnel including program office personnel, IT Operations personnel, HUDCIRT, the Office of General Counsel and the Inspector General.

1. Gather incident data
2. Conduct Analysis and Assessment
3. Work with the program area experiencing the incident:
   - To determine how to quickly contain the incident
   - To develop a response strategy
   - How quickly the strategy can be implemented
4. Ensure documentation of the incident is updated
5. Take steps to prevent any further incidents

If HBNRT is not convened mitigation must still be *reviewed (Continue to Mitigation Section to review steps).*

6.5 If the Impact Level is determined to be Impact Level 1 (High):

- The Privacy Officer and CISO notify SAOP of their determination that the privacy incident is Impact Level 1
- The Privacy Officer updates the Breach Incident Report Form
- SAOP notifies the HBNRT within 24 hours of being notified of the Impact Level 1 Breach.
- The SAOP shall convene a meeting of the complete HBNRT or specific members as needed and identified through the conduction of the Preliminary Risk Assessment.
- The HBNRT reviews the following:
  1. Information gathered in the preliminary investigation
  2. Privacy Risk Management Worksheet
  3. Breach Incident Report

7. Full Risk Assessment

Once it has been decided by the SAOP based on the recommendations from the Privacy Officer and CISO to convene the HBNRT, the team will conduct a full risk assessment to determine the full extent of harm that may be caused from the incident. The CIO in consultation with the HBNRT will provide the final risk-assessment rating.

7.1 Incident Classification

It is important to understand first what type of incident has occurred and what areas of privacy may be affected. The following classifications derive from a variety of sources (see References). A privacy incident is a violation of one of the following:

1. Agency Policies and Procedures regarding
   a. U.S. Department of Housing and Urban Development Investment Strategy, Policy and Management Standard Operating Procedure "Guidelines and Administrative Procedures for Departmental Privacy Program Office"
   b. Privacy Act Handbook (1325.1)
   c. US Department of Housing and Urban Development Breach Notification Policy and Response Plan
   d. IT Security Manual 2400.25
2. Notice/Awareness – Notice is the practice of providing clear information to individuals, whose information is collected, regarding privacy practices governing the collection, use, disclosure, and retention of personally identifiable information. Awareness is the method(s) of making that notice available to individuals.
3. Limitation – Ensuring that the personally identifiable information collected for the stated purpose is absolutely necessary (i.e., minimal) and that personally identifiable information is used only for the stated purposes for which it was initially collected
   a. Limitation of Use - The organization uses personally identifiable information only for the intended purpose for which the information was originally collected.

b. Limitation of Collection - The organization collects only the personally identifiable information that is necessary and relevant to the purpose for which the information is collected.

c. Limitation of Retention

i. Retains personally identifiable information only for as long as necessary to fulfill the intended purpose for which the information was originally collected;

ii. Properly destroys and disposes of personally identifiable information that is no longer needed to fulfill its intended purpose, in accordance with applicable laws, directives, policies, and regulations; and

iii. Provides notice if personally identifiable information must be retained longer than it is needed to fulfill its intended purpose.

4. Sharing and Disclosure

a. Discloses and shares personally identifiable information only with those individuals and organizations needing such information to perform official duties and for the intended purpose for which the information was originally collected, unless otherwise directed by applicable laws, directives, policies, or regulations;

b. Makes individuals and organizations receiving the personally identifiable information aware of the limitations on the use, disclosure, and retention of the information.

5. Accuracy – Ensuring personally identifiable information is correct when collected and is updated periodically to maintain correctness. Accuracy of personally identifiable information is necessary to ensure that individuals are treated appropriately in decisions (e.g., legal, personnel, financial, criminal) based on their personally identifiable information.
6. Choice/Consent - Providing individuals with the ability to consent to the collection, use, disclosure, and retention of their personally identifiable information.
7. Access, Redress, and Correction – Providing individuals with the ability to review personally identifiable information held about them, have their concerns about their information addressed, and have their information corrected.

7.2 Potential Impact of Harms

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 (as described in section 3.7) are due primarily to privacy violations, but can also be due to ambiguous identification, erroneous authentication, and/or inaccurate authorization.

Table 7-1: Examples of Appropriate Selection of Privacy Impact Levels

Potential Impact Levels	Social Harm	Physical Harm (includes mistreatment or distress)	Financial Harm
Low: The failure to satisfy one or more of the privacy principles could be expected to have a limited adverse effect on individuals.	Short-term and limited-scope inconvenience, embarrassment, distress, or damage to personal standing or reputation; limited increased vulnerability to social engineering; limited increased vulnerability to extortion (e.g., traveler data)	Minor injury or health impact or short-term and limited-scope physical inconvenience (e.g., delay/missing flight because of misidentification at airport security check point)	Limited loss or liability, damaging short-term financial liability (e.g., identity theft results in the individual having to incur short-term debt or having credit applications rejected)
Moderate: The failure to satisfy one or more privacy principles could be expected to have a serious adverse effect on individuals.	Significant short-term or limited long-term inconvenience, embarrassment, distress, or damage to personal standing or reputation; significant increased vulnerability to social engineering; significantly increased vulnerability to extortion (e.g., revelation of arrest records, such as DWI).	Significant risk of minor injury or limited risk of injury requiring medical treatment; or serious short-term or limited long-term physical inconvenience (e.g., victim of vigilantism due to release of false/incomplete police report)	Significant loss or liability, damaging long-term financial liability (e.g., identity theft results in the individual incurring long-term or significant debt)
High: The failure to satisfy one or more privacy principles could be expected to have a severe or catastrophic adverse effect on individuals.	Severe and lasting distress or damage to personal standing or reputation (e.g., revelation of sensitive medical history, such as HIV) to a large number of individuals or to a small number of very highly placed individuals (e.g., scandal involving senior executives adversely impacting ability of organization to function);	Risk of serious injury or death or severe and lasting physical distress (e.g., false arrest and conviction; public identification of an individual in a Witness Protection Program)	Severe or catastrophic consequences (e.g., identity theft results in bankruptcy, criminal liability) to a large number of individuals

7.3 Privacy Impact Level

Table 7-2: Privacy Impact Levels

Privacy Impact Level	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 impact level:

Potential Impact Level	Definition	Examples
Level 3 (Low)	• No sensitive PII involved • Low impact (distress, inconvenience or corrective action) to affected individuals • Minimal corrective action required by HUD	• A 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.
Level 2 (Moderate)	• No sensitive PII involved • Moderate impact (distress, inconvenience, or corrective action) to affected individuals • Significant corrective action possibly required by HUD	• 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.
Level 1 (High)	• Sensitive PII involved • Potentially high impact (distress, inconvenience or corrective action) by affected individual(s) • Potentially adverse effect on organizational operations, assets, reputation, and affected individuals	• A file with detailed information depicting the income levels of housing recipients, including name, SSN, 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.

7.4 Part 2: Incident Classification and Potential Harms

Complete the Privacy Risk Management Worksheet below indicating the information that is at risk, and the potential harms from the loss.

Privacy Risk Management Worksheet

Part 1: Identify PII and Transactions that Involve PII

In the box provided below, describe the transaction(s) where PII is collected, used, and/or retained.

Description of transaction:

Using the list of PII below, place a check next to the types of PII collected, used, and/or retained in the transactions described above (select all that apply)

Identification Information	Identification Numbers	Financial Information	Other Type of PII
☐ Name ☐ Date of birth ☐ Place of birth ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video)	☐ Social Security Number (or other number originated by a government that specifically identifies an individual)	☐ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☐ FHA Number	☐ Other (if checked, list the type of PII)

Identification Information	Identification Numbers	Financial Information	Other Type of PII
☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☐ Mother's Maiden Name ☐ Mailing Address ☐ Phone Numbers (e.g., phone, fax, and cell) ☐ E-mail Address	☐ Certificate/license numbers (e.g., Driver's License Number) ☐ Vehicle Identifiers (e.g., license plates) ☐ Passport number ☐ Alien (A-) number		

Part 2: Identify Potential Harms and Their Levels

In the table below, identify potential harms for the PII transactions and what the levels of harm are. The overall potential harm is the highest level of harm indicated among the three types of harms (social, physical, and financial).

Social Harm			Physical Harm			Financial Harm			Overall Potential Harm		
Low ☐	Mod ☐	High ☐	Low ☐	Mod ☐	High ☐	Low ☐	Mod ☐	High ☐	Low ☐	Mod ☐	High ☐

7.5 Investigation Method

The CIO, in consultation with the HBNRT, should limit internal notifications and access to individuals who have a legitimate need to know. The HBNRT should review what has happened as follows:

- Document the investigation and gather all information necessary to describe and address the incident.
- Review the Privacy Incident Report submitted to US-CERT and identify any additional information necessary.
- Confirm what personal information is lost or at risk.
- Identify the steps taken to reduce the risk of harm.

The HBNRT must identify the lead investigator for a particular privacy incident. The lead investigator should be someone who is trained in, or familiar with, incident response procedures and the complexities involved with the potential loss or compromise of PII.

The lead investigator should consult with the HUD Office of the Chief General Counsel before initiating investigation on issues pertaining to the handling of evidence and chain of custody.

7.5.1 Investigators' Plan of Action

The lead investigator will

- Create and maintain a chain-of-custody log of all personnel who have access to the evidence. Investigators keep a record of the individuals who have touched each piece of evidence. The record should include the date, time, and locations of where the evidence is stored.

The OIG and HUD CIO will

- Notify external law enforcement, where criminal activity is suspected or confirmed, depending on level and severity of criminal activity.
- Notification and involvement of external law enforcement must be documented in the Breach Incident Report.

Law enforcement then consults with the lead investigator and other HBNRT members, as warranted. In incidents in which criminal activity is suspected or confirmed, the lead investigator consults with law enforcement, OIG, and the HUD Deputy Secretary regarding the closure of the investigation.

Investigators review events and actions at the conclusion of the investigation and make recommendations to the HBNRT, Human Capital Officer, General Counsel, Customer Relations Manager, Chief Procurement Officer and the Deputy Secretary as necessary.

Privacy incidents designated as low-impact do not require the continued involvement of the HBNRT. The PO and CISO will handle the closure of the incident and report the results to the SAOP in accordance with Section 9 Mitigation and Section 10 Closure.

If a moderate or high-impact privacy incident is involved, the SAOP will report the findings to the Chief Operating Officer, Office of Inspector General, Human Capital Officer, General Counsel, Customer Relations Manager, Chief Procurement Officer and the Deputy Secretary. The report will also be given to the Program Manager of the program experiencing the breach.

The lead investigator sends a copy of any investigation report(s) by email to HBNRT members if a HBNRT is convened. If no HBNRT is convened, the Privacy Officer/CISO sends any report(s) by email to the SAOP.

Upon completion of the investigation, the Privacy Officer/CISO updates the Privacy Incident Report to indicate the closure of the investigation, subject to review by the SAOP.

8. Notification

8.1 Notification of Individuals

The HBRNT shall base their recommendations for providing external notification on:

- Accessibility. Whether the information is easily accessible by malicious actors or whether it is encrypted, password protected, or protected by physical security measures
- Sensitive in combination. Whether the affected personal information, such as external information on race, religion, national origin, family status, disability, health or finances, can be combined with other available information to become sensitive.

The CISO should provide an assessment to the CIO on the accessibility of the information.

The CIO in consultation with the HBNRT will make a final decision on whether external notification will be provided. HUD Privacy Officer records decision in the breach incident report.

Notification of Individuals is necessary for any Privacy-related incident where individuals have been identified. Notice shall be provided without unreasonable delay but no later than 45 days after a risk of harm analysis has been made.

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

8.2 Determine Source of Individual Notification

Notifications to affected individuals shall generally be issued by the Secretary or by a senior-level individual that he/she may designate in writing (typically the Assistant Secretary of the program office experiencing the breach). The exception is for incidents involving less than 50 individuals. The Department can designate the HUD CIO and HUD Privacy Officer as the notifying officials when less than 50 individuals are affected. In such cases, the CIO and Privacy Officer work with the program office experiencing the breach to confirm the names and addresses of the individuals affected as well as the contents of the notification, and the timing.

When the breach involves a Federal contractor or an organization operating a Departmental system of records on behalf of the Department, the Department shall be responsible for ensuring or issuing a breach notification in accordance with the Breach policy.

The CIO in consultation with the HBNRT makes a final decision as to who will provide external notification. HUD Privacy Officer records decision in the Privacy Incident Report.

Table 8-1: Source of Individual Notification Checklist

Source of Individual Notification	Yes	No
1. Does the privacy incident involve a limited number of individuals (e.g., under 50)?	☐	☐
a. If yes, the HUD CIO and HUD Privacy Officer issue individual notification jointly		
b. If no, the HUD Secretary or designee issues the individual notification unless another exception applies. Continue to the next question.		
2. Does the privacy incident involve a federal contractor or a public-private partnership, "Third Party", operating a system of records on behalf of the agency?	☐	☐
a. If yes, is HUD the primary data owner, as evidenced by Memoranda of Agreements or other legal program documents?	☐	☐
i. If yes, then the HUD Secretary or designee issues the individual notification or HUD Secretary must issue written notification that appoints a person as the Secretary's official designee for addressing privacy incident response.		
ii. If no, then the federal contractor or third-party is responsible for providing individual notification to affected party(ies). The roles, responsibilities, and relationships with contractors or partners should be reflected in the system certification and accreditation (C&A) documentation, as well as contracts and other documents. The Third Party issues the individual notification.		
b. If no, then the federal contractor or third-party is responsible for providing individual notification to affected party(ies). The roles, responsibilities, and relationships with contractors or partners should be reflected in the system certification and accreditation (C&A) documentation, as well as contracts and other documents.		

8.3 Create Content for Individual Notification

The HUD Privacy Officer drafts content for notification and delivers the draft to the HBNRT.

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.
- Contact information of the Deputy Assistant Secretary of Public Affairs for affected individuals to contact for more information, as well as a toll-free number, TTY number, website, and/or postal address.

Notices shall *not* include

- Any specific PII concerning the affected individuals. The notice can include only the type of PII.

The CIO in consultation with the HBNRT reviews the notification letter prior to its distribution.

If the breach involves individuals for whom English is not their native language, efforts will be made to translate notifications into appropriate languages.

If the breach response includes a Website notice, such notices shall be 508-compliant.

If the individuals affected by the breach include individuals with visual or auditory impairments, TTY numbers shall be provided.

Table 8-2: Individual Notification Content Checklist

Does the Individual Notification:	Yes	No
1. Include a brief description, including date(s) of the breach and of its discovery	☐	☐
2. Identify the types of PII and related information involved?	☐	☐
3. State 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?	☐	☐
4. Describe the steps individuals should take to protect themselves from potential harm?	☐	☐
5. Inform the individual of the steps the Department has underway to investigate the breach, to mitigate losses, and to protect against any further breaches?	☐	☐
6. Provide contact information of the Deputy Assistant Secretary of Public Affairs for affected individuals to contact for more information, including a toll-free number, TTY number, website, and/or postal address?	☐	☐
7. Include only the type of PII and not any specific PII concerning affected individuals?	☐	☐
8. Comply with 508 requirements?	☐	☐
9. Include a TTY number provided for affected individuals with visual or auditory impairments?	☐	☐

8.4 Determine Means of Individual Notification

The HBNRT works with the official responsible for notification to determine how and when notification will be provided. Factors to consider in this deliberation include:

- **Urgency.** Notification should be urgent if the potential harm can be mitigated by quick action, e.g., providing a credit report, registering for credit monitoring, etc. If the harm cannot be mitigated, notice should be provided within a reasonable timeframe, not to exceed forty-five (45) days from determination of the risk of harm.
- **Involvement of Law Enforcement.** If the privacy incident involves law enforcement activities, notification should be made within a reasonable timeframe, not to exceed forty-five (45) days once it is established that notification will not impede or inhibit investigation.
- **Adequacy of Contact Information.** If adequate information exists, notification should be provided by U.S. Postal Service First Class Mail. In urgent situations, notice may be provided by telephone, so long as notification is also associated with written notification delivered by first-class mail. Notification by email may be appropriate in situations where an individual has provided an email address to HUD and has expressly given consent to email as the primary means of communication with HUD, and no known mailing address is available.
- **Number of Affected Individuals.** When an incident involves a large number of individuals, substitute notice may be provided through government provided services, such as USA Services, 1-800-FedInfo; public media such as television and newspapers, particularly in the market serving affected individuals; and HUD websites. Notice to media should include a toll-free phone number where an individual can learn whether or not his/her personal information is included in the privacy incident.

The HUD Privacy Officer records decision related to how and when notification will be provided in the Breach Incident Report.

Table 8-3: Matrix for Means of Notification

		Number of Affected Individuals					
		0-500		500-500,000		500,000	
		Adequate	Inadequate	Adequate	Inadequate	Adequate	Inadequate
Urgency	Urgent	• USPS Email • Telephone	• Email	• USPS Email • Telephone	• Email	• USPS	• Government-provided services • Public media • HUD website
	Not Urgent	• USPS	• HUD website	• USPS	• Public media • HUD website	• USPS	• Government-provided services • Public media • HUD website

8.5 Coordinate Internally

The HBNRT will coordinate via email or voicemail with the following HUD internal stakeholders prior to providing external notification:

- HUD Public Affairs Office

- HUD Senior Officials
- HUD Legislative Affairs

Table 8-4: Internal Coordination Checklist

Has the notification been coordinated with:	Yes	No
1. HUD Senior Officials?	☐	☐
2. HUD Public Affairs?	☐	☐
3. HUD Legislative Affairs?	☐	☐

If the incident is a Privacy Incident Impact Level 1 (High) privacy incident, the HUD Legislative Affairs Office and HUD Public Affairs Office coordinate notification to the appropriate Congressional committee chair(s). This notification is issued in advance of or simultaneously with the issuance of a press release or notification to affected individuals.

8.6 Determine Need for Third Party Notification

Based on the nature of the breach, the CIO in consultation with the HBNRT shall determine the need to notify any third parties based on the following checklist.

Table 8-5: Third Party Notification Checklist

Third Party Notification	Yes	No
1. Are there any criminal violations relating to the disclosure or use of PII and Covered Information?	☐	☐
If yes, 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.		
2. Does the privacy incident require communications with members of Congress and their staffs?	☐	☐
If yes, the HBNRT shall notify the Assistant Secretary for Congressional and Intergovernmental Relations immediately. 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.		
3. Does the privacy incident involve government-authorized credit cards or individuals' bank account numbers that are used in employment-related transactions (e.g., payroll)?	☐	☐
If yes, the CFO in consultation with the HBNRT shall promptly notify the bank or other entity that is responsible for the particular transaction.		
4. Do the privacy incident mitigation or notification processes require communication with or through the press?	☐	☐
If yes, the General Deputy Assistant Secretary for Public Affairs, in coordination with the HBNRT, shall direct 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.		
5. Do the privacy incident mitigation or notification processes require communication with vendors or other third parties related to the incident?	☐	☐
If yes, the HBNRT shall notify the Customer Relationship Manager, who will review contracts related to effected vendors for security obligations, responsibilities for mitigation costs, proper roles and responsibilities, and accountability procedures. They will also consult with the Privacy Officer in developing communication with affected/implicated vendors regarding obligations to protect PII, and obligations to participate in incident investigation, containment, and mitigation		

8.7 Provide Notification

After the CIO in consultation with the HBNRT has approved content of notification to affected individuals, coordinated with internal stakeholders, and notified appropriate third parties, HUD provides notification to affected individuals from the previously determined HUD source.

The HUD Privacy Officer updates the Breach Incident Report with copies of the notice provided.

9. Mitigation

9.1 Purpose of Mitigation

HUD must be prepared to act quickly to minimize the potential harm to individuals that can result from a privacy incident. While assessing the risk of a particular incident, HUD should simultaneously take steps to begin mitigating the potential harm to individuals. It must be remembered that a wide range of harms may be caused by a privacy incident and subsequent mitigation actions should take the broadest possible view of potential harm.

Mitigation consists of the actions essential to:

- Containing the incident,
- Eradicating the incident,
- Identifying and mitigating all vulnerabilities that were exploited,
- Enacting countermeasures to minimize subsequent harm,
- Restoring the impacted systems, electronic or physical, or data stores back to an operational state, and
- Implementing, if necessary, additional monitoring to look for future related activity.

9.2 Timing and Sequence

For Impact Level 1 breaches, mitigation activities occur in coordination with Reporting, Escalation, and Notification. Decisions made during Mitigation activities must be made in concert with these parallel phases to ensure minimization of harm to impacted individuals.

9.3 Mitigation Responsibilities

Mitigation activities are directed by the Privacy Officer, CISO and IT Security office, HUDCIRT, and IT Operations, the Office of General Counsel and Office of Inspector General depending on the nature of the privacy incident.

Depending on the nature of the privacy incident and the type of harm to be offset, additional departments and individuals will be involved in execution of Mitigation activities. Parties who should be prepared to participate include

- Third party organizations involved with the incident
- The Program Manager of the Program experiencing the breach
- The HUDCIRT to recommend technical resolutions and containment strategies
- The System Manager for any technical system involved or potentially threatened
- The Manager of physical security for any compromised locations.

- The Chief Procurement Officer for ordering of any credit monitoring services.
- The Chief Human Capital Officer for breaches involving employee misconduct

For Impact Level 1 breaches, the Privacy Officer and the CISO will inform the HBNRT of all mitigation activities, and the HBNRT will provide final approval regarding certain decisions related to engagement of external law enforcement.

Throughout the execution of this procedure, all mitigation measures for Impact Level 1 and 2 incidents must be documented in the Service Desk Ticket, and the Breach Incident Report.

9.4 Incident Containment

At the time an incident is reported, it is vital to ensure that there is no additional loss or compromise of information. The Privacy Officer, CISO, IT Security work with any other applicable party to contain the incident.

- The Program Manager of the area involved in the incident must gather and secure evidence of the incident, in accordance with direction from PO, CISO, Office of General Council (OGC), Office of Inspector General (OIG), or in the event of a technology related event, in accordance with directions from HUDCIRT and IT Operations.
- Best practices for containing an incident include:
  - Not printing or forwarding emails regarding the event,
  - Physically securing under lock any vulnerable information, and
  - Minimizing disclosure or knowledge of the potential privacy incident.
- The HUDCIRT analyzes the evidence and collaborates with the Program Manager regarding the identification of the source of the incident and the implementation of appropriate measures to contain information loss.
- The HUDCIRT additionally analyzes the cause of the incident to determine if larger corporate threats exist.
- Based on the analysis of both the immediate issue and any larger threat, the Privacy Officer, CISO, and IT Security will work with the appropriate teams to ensure the impacted systems or data collections are secured and the vulnerability is isolated.
- If it is determined that the threat could be recurring, then the CISO, IT Security and the Privacy Officer should implement the appropriate ongoing monitoring strategies.

9.5 Countermeasures to Minimize Harm

As the source of the loss is stabilized, and the HBNRT completes its assessment of the likely risks of harm, the HBNRT will identify countermeasures the Department can implement to minimize any further risk of harm to individuals. The HBNRT may direct a subset of members or personnel within the program office to identify countermeasures and a plan for implementing such measures.

It is important to remember that there are different types of harms, and therefore, different countermeasures needed based on the situation. In many cases, a broad range of countermeasures may be required as dictated by the nature and sensitivity of the PII.

As the plan for countermeasures is developed, the HBNRT should review the recommended plan of action, initiate additional phases of activity and ensure adequate funding is available if needed for any of the recommended steps.

Additionally, the decision of which countermeasures are appropriate should take into account both the objective of minimizing harm to individuals related to the immediate incident, as well as any longer term activities that could have the potential for precluding similar incidents in the future.

Finally, the Privacy Officer and CISO should document any implemented mitigation countermeasures in the Breach Incident Report. If Notification to impacted individuals is required, the list of implemented countermeasures should be communicated to the team managing those notifications for consideration of inclusion in the notification letter.

Listed below is a sampling of different types of Mitigation countermeasures. This list is by no means exhaustive. The specific set of countermeasures selected will be based on the nature of the incident and the Risk of harm Analysis.

- Notification of affected individuals, the public, and other government entities (e.g. Congress) pursuant to the Notification section of this document.
- Removing exposed information from an Internet or Intranet page.
- Notification of external law enforcement (subject to notification and concurrence by the HBNRT) in coordination with the Investigation and Notification phases.
- Contacting appropriate financial institutions for incidents involving credit cards.
- Offering of initial credit report, additional credit monitoring, or identity-theft monitoring services to mitigate the misuse of PII and to identify patterns of suspicious behavior.
- Agency review of decisions regarding individuals, in cases where data or perspectives used to make decisions may have been compromised due to the incident.
- Determination of destruction of any exposed material (subject to approval from General Counsel and Records Management based on agency procedures for handling exposed material).

9.5.1 Ordering Credit Monitoring

If the HBNRT determines that credit monitoring services are necessary for a particular suspected or confirmed privacy incident, the Chief Procurement Officer should follow OMB Guidelines M-07-04 *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)* dated December 22, 2006.

The process begins with a review of the pricing and terms and conditions of the GSA BPAs, in addition to any other credit monitoring services that the Chief Procurement Officer is considering in their market research.

If the Chief Procurement Officer decides to order credit monitoring through GSA, then the Chief Procurement Officer follows the ordering procedures as defined in OMB M-07-04.

(a) The applicable services shall be Special Item Numbers (SIN) 520 16 Business Information Services.

(b) Prepare a Statement of Work (SOW) that includes, at a minimum, work to be performed, location of work, period of performance, deliverable schedule, applicable performance standards, and any special requirements.

(c) Prepare a Request for Quotation (RFQ) to include at a minimum the SOW and evaluation criteria.

1) *Orders at or below the micro purchase threshold.*

(i) Orders may be placed at or below the micro-purchase threshold ($2500) with any BPA-holder. Attempt to distribute orders at or below the micro-purchase threshold among all BPA holders.

2) *Orders exceeding the micro-purchase threshold.*

(i) Develop an SOW in accordance with the instructions stated above.

(ii) Provide the RFQ (including SOW and evaluation criteria) to at least three BPA-holders.

(iii) Request that BPA-holders submit firm-fixed prices to perform services identified in the SOW. This does not preclude the use of Labor Hour or Time and Material (T&M) task orders.

3) *Orders exceeding the maximum order threshold of $1,000,000.*

(i) Provide the RFQ (including SOW and evaluation criteria) to additional BPA-holders. When determining the appropriate number of BPA-holders, consider, among other factors, the following:

A. The complexity, scope and estimated value of the requirement.

B. The market search results.

(ii) Seek price reductions.

4) Provide the RFQ (including the SOW and evaluation criteria) to any BPA-holder that requests a copy of it.

(d) Evaluate all responses received using the evaluation criteria provided to the BPA-holders. Any ordering agency is responsible for considering the level of effort and the mix of labor proposed to perform specific tasks being ordered, and for determining that the total price is reasonable. Place the task order with the BPA-holder that represents the best value (see FAR 8.404 (d)). After award provide timely notification to unsuccessful BPA-holders. If an unsuccessful BPA-holder requests information on an award that was based on factors other than price alone, provide a brief explanation of the basis for the award decision.

(e) Document the following:

1) The BPA-holders considered, noting the BPA-holder from which the service was purchased;

2) A description of the service purchased;

3) The amount paid;

4) The evaluation methodology used in selecting the BPA-holder to receive the task order;

5) The rationale for any tradeoffs in making the selection;

6) The price reasonableness determination required by paragraph (d) of this subsection; and

7) The rationale for using other than—

   (i) A firm-fixed price task order; or

   (ii) A performance-based task order.

If the Chief Procurement Officer decides to order credit monitoring other than through the GSA BPAs, then HUD must notify the GSA with a copy to the OMB E-Government Administrator that explains how the proposed contract offers a better value to HUD. This notification must identify the pricing and the terms and conditions. The Chief Procurement Officer must coordinate the notification with the CIO, and submit the notification to the GSA at least 10 days prior to making the award. In the event of unusual or compelling urgency, the notification can be provided as soon as is practicable.

9.6 Breach Involving a Disruption of Services to Information System or Data Store

After the immediate threat has been contained, and while the other phases of the HBNRP is underway, the CIO must plan and lead the activities required to resume the regular operations of the impacted Program. Normal activities cannot begin, however, until the system or data store that was breached has been re-secured, and the integrity of the system has been confirmed.

For technical systems, restoration of an affected system requires its being brought back to an operationally ready state where the system is functioning normally. The Privacy Officer, CISO, IT Security, and the owner of the impacted system will work jointly to determine the appropriate steps for restoring the integrity of the compromised technical system.

9.7 Compromises of Paper-Based Systems

For compromises of paper-based systems, the confirmation of the security of the remaining documents in the data store, along with the restoration of appropriate physical security measures, must be assured to restore the integrity of the system. The Privacy Officer will work jointly with the Program owner of the impacted data store and with the CIO to ensure security is re-established for the affected data store.

10. Closure

Completion of the investigation of the incident warrants closure of a Privacy Incident, the issuance of external notification (if needed), and the implementation of all suitable privacy and IT security mitigation measures.

HUDCIRT will follow normal incident-response procedures to close out Service Desk tickets and will notify PO of the ticket closure.

All Level 3 incidents can be closed by following normal incident response procedures. For incidents that require the involvement of the HBNRT, the PO should follow up with all of the members of the team to make sure that all of the action items have been completed and there is a record (e.g., via email) providing confirmation of completeness. The Privacy Officer will also update the Breach Incident Report to recommend incident closure, subject to review by the CIO.

11. Supplemental Activities

Supplemental activities provide organizations the ability to ensure they are better prepared for future incidents.

11.1 Activities

- The Privacy Officer and CISO will identify and post lessons learned on Privacy Intranet Website or as a formal document to be distributed to the members of the HBNRT.
- Privacy Officer collects and updates point of contact information concerning members of the HBNRT, senior officials and any other officials required to be notified.
- Members of the HBNRT and other HUD senior officials as designated are responsible for conducting an annual review of the implementation of the Breach Notification Response Plan which will include the following:
  - Review of Privacy Incidents that occurred during the preceding 12-month period and the manner in which they were handled;
  - Identification of Privacy Incident handling procedures and practices that must be revised in order to strengthen DHS safeguards for PII;
  - Identification and adoption of best practices that must be incorporated in the Privacy Breach SOP; and
  - Examination of training programs pertaining to the implementation of the Privacy Breach SOP and the safeguarding of PII.

The Privacy Officer will chair the review process and will prepare the Annual Report for the Program Review of the Breach Notification Response Plan.

11.1.1 Lessons Learned

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Many organizations have found that holding a “lessons learned” meeting with all involved parties after a major incident, and periodically after lesser incidents, is extremely helpful in improving security measures and the incident handling process itself. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the lessons learned meeting include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?

- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Small incidents need limited post-incident analysis; it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the incident that is being analyzed, but also it is wise to consider who should be invited for the purpose of facilitating future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting increases the likelihood that the participants' needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it is also important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Lessons learned meetings provide other benefits. Reports from these meetings are good material for training new team members by showing them how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the lessons learned process. Post-mortem analysis of the way an incident was handled will often reveal a missing step or an inaccuracy in a procedure, providing impetus for change. Because of the changing nature of information technology and changes in personnel, the incident response team should review all related documentation and procedures for handling incidents at designated intervals.

Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use. First, the report provides a reference that can be used to assist in handling similar incidents. Creating a formal chronology of events is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident may have caused This estimate may become the basis for subsequent prosecution activity by entities such as the U.S. Attorney General's office. Follow-up reports should be kept for a period of time as specified in record retention policies.

11.1.2 Using Collected Incident Data

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If

incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team.

Appendix A. Illustrations of Privacy Incidents

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

Insufficient Notice

1. An individual submits personal financial information for a loan after being informed that their information is necessary for the loan application. In addition to being used to assess the loan application, the individual's financial information is shared with a research organization in an attempt to identify possible indicators of fraud.
    - Mitigation: Privacy Office verifies that the authority for collecting financial information allows for its disclosure to research organizations. Privacy Office also reviews relevant legal agreements to ensure that limits are established for the use and third-party disclosure of the information shared, and that security requirements are established to protect the information. The Privacy Office collaborates with the Program Office and the Records Management Office to ensure that the Privacy Act Statement associated with the initial collection of financial information describes all authorities and uses of the information collected.
2. A Program Office develops an Access database, in which records are retrieved by personal identifier, to automate a manual process outside of formal system development procedures.
    - Mitigation: Program Office collaborates with the Privacy Office to publish a System of Records Notice in the Federal Register that covers the Access database. The SORN must provide notice to the public about the existence of the system, identify the authority for the system, and describe how the information maintained by the system is used, shared, protected, and retained. The Privacy Office also collaborates with the Program Office to conduct and publish a Privacy Impact Assessment that evaluates the impact of automating a previously manual process on an individual's privacy.

Insufficient Redress

1. An individual contacts HUD to complain about how their personal information is being handled.
    - Mitigation: The Privacy Office collaborates with the Program Office to determine the validity of the compliant, in particular, assessing whether sufficient notice regarding the use of personal information was provided to the individual, whether there are sufficient opportunities to correct the personal information that may be at issue, and the relevance of existing appeals process to address the complaint. If sufficient opportunities exist, the Privacy Office works to ensure that the complaint is addressed. If sufficient opportunities do not exist, the Privacy Office works with appropriate department offices to establish policy and procedures necessary for adequate redress.

Loss of Control

1. 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.

- Mitigation: While continuing efforts to locate the lost thumb drive, the Privacy Office collaborates with the Program Office to identify the individuals that could be affected to support notification procedures and to determine the appropriateness of re-issuing badges.

2. A supervisor reports 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**.
   - Mitigation: Privacy Office and Information Security Office investigate to determine the likelihood that the personal information was compromised. The Privacy Office also collaborates with the affected Program Office to identify affected individuals, and provide notification of the incident.

Compromise

1. 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.
   - Mitigation: The Privacy Office collaborates with the Physical Security Office to restore security to the file cabinet or find an alternate location to secure the files. The Privacy Office also collaborates with the Chief Financial Office, if the financial records are related to the organization's employees, and the Chief Procurement Office, if credit monitoring services will be provided to affected individuals. The Privacy Office works with the Program Office to identify any affected individuals prepare a notification letter and detail the provision of credit monitoring services.

Unauthorized Disclosure

1. 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.
   - Mitigation: Privacy Office provides notification to the affected individual and describes the procedures that will prevent future occurrences from happening.
2. Security clearance documents containing the sensitive **PII** of employees were faxed in error to the wrong agency's security office.
   - Mitigation: Privacy Office coordinates with the erroneous recipient of the security clearance documents to ensure that the documents are returned without further disclosure. The Privacy Office also coordinates with Chief Human Capital Office to create a record of the incident in personnel and security files so that no arbitrary, negative impact to the affected individuals occurs. The Privacy Office works with General Counsel and Records Management, who determine whether the exposed material should be destroyed based on agency procedures for handling exposed material.

Unauthorized Acquisition

1. An employee uses another employee's password and pin to copy **government credit-card numbers and Personal Identification Numbers**.
   - Mitigation: Privacy Office collaborates with Chief Human Capital Office prior to taking action that affects employees, notifies the Office of Inspector General to determine

whether external law enforcement should be contacted, and works with the Office of Chief General Counsel to manage the investigation and address issues pertaining to the handling of evidence and chain of custody. Privacy Office also notifies the Chief Financial Office, so that the Chief Financial Office can begin monitoring the use of government credit cards and consider the necessity of reissuing affected cards. If there is a risk of identity theft, the Privacy Office contacts the Chief Procurement Office to establish credit monitoring services. Consequences to the individual may include removal of all system access, formal reprimand, criminal charges, or termination.

2. A visitor takes a file containing the **names, credit reports, authorization files, and signatures** of employees that she finds in a conference room.
    - Mitigation: Privacy Office identifies the affected individuals and notifies them of the compromise of their information. If there is a risk of identity theft, the Privacy Office contacts the Chief Procurement Office to establish credit monitoring services. The Privacy Office also works with the Physical Security Office to assess access procedures to the conference room and address any deficiencies. The Privacy Office also works with the Chief Human Capital Office to create a record of the incident in personnel files so that any negative impact to the affected employees can be mitigated.

Unauthorized Access (Internal and External)

1. A contractor misuses administrator privileges to view sensitive information on **contract bids, government procurement-card numbers, and tax identification numbers**.
    - Mitigation: Privacy Office collaborates with Chief Human Capital Office prior to taking action that affects employees, notifies the Office of Inspector General to determine whether external law enforcement should be contacted, and works with the Office of Chief General Counsel to manage the investigation and address issues pertaining to the handling of evidence and chain of custody. Privacy Office also notifies the Chief Financial Office, so that the Chief Financial Office can begin monitoring the use of government procurement cards and consider the necessity of reissuing affected cards. If there is a risk of identity theft, the Privacy Office contacts the Chief Procurement Office to establish credit monitoring services. Consequences to the individual may include removal of administrative privileges, additional training on the proper use of systems, removal of all system access, formal reprimand, criminal charges, or termination.

Appendix B. Sample Notification Letter

[Date]

Dear _____,

This letter is to inform you that **[Insert description of document, system, or device]** containing personally identifiable information (PII) about you was **[lost/stolen/compromised]** on **[Insert date of incident and/or detection of incident]**. We apologize for this **[loss/error]** and want to assure you that we are diligently working to prevent this situation from occurring again. [**If applicable, insert an explanation as to whether the HUD CIO believes that the information will remain confidential]. [Explain whether security controls like password-protection, encryption, etc., were used and what steps have already been taken to reduce the risk of harm]. [Describe actions taken by agency (e.g.., referred to external agency or local police) for investigation**]. Appropriate steps are being taken to mitigate the loss of your PII and to prevent any further incidents.

As a precaution, you may wish to consider taking the following steps:

- First, you may wish to consider placing a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call any one of the three credit reporting agencies at the phone numbers listed below.

Credit Reporting Firm	Telephone Number
Equifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

You should

1. Request that a fraud alert be placed on your account; and
2. Order a free credit report from the agency.

We recommend that you request a free credit report from each agency with a 4-month interval between requests. In other words, make a request to one agency, wait four months, then submit a request to the next agency, and so on. You should continue to do so for a period of 12-24 months.

- When you receive your credit reports, review them carefully for accounts that you did not open or for inquiries from creditors that you did not initiate. Also, review your PII for accuracy. If you see anything that you do not recognize or understand, you should immediately call the credit agency at the number on the report.
- Third, if you find any suspicious activity on your credit reports, promptly file a report with your local police office and the Federal Trade Commission (FTC). Suspicious activities could include the following:
  - Inquiries from companies you have not contacted or done business with;
  - Purchases or charges on your accounts you did not make;
  - New accounts you did not open or changes to existing accounts you did not make;

- Bills that do not arrive as expected;
- Unexpected credit cards or account statements;
- Denials of credit for no apparent reason; and
- Calls or letters about purchases you did not make.

For additional information on identity theft, you may wish to visit the FTC's Identity Theft web site at http://www.consumer.gov/idtheft/.

Please be alert to any phone calls, emails, and other communications from individuals claiming to be from the Department of Housing and Urban Development or other official sources, asking for your personal information or asking to verify such information. This is often referred to as information solicitation or "phishing." **Neither HUD nor [Third Party Associate] will contact you to ask for or to confirm your personal information.**

The officials and employees of the Department of Housing and Urban Development take our obligation to serve our citizens very seriously, and we are committed to protecting the information with which we are entrusted. In response to incidents like this and the increasing number of data breaches in the public and private sectors, the Department is continuously monitoring its systems and practices to enhance the security of personal and sensitive information.

We sincerely apologize for any inconvenience or concern this incident may cause you. If you have questions regarding this letter, please contact **[Insert POC Name], [Insert Component and Position Title], at [Insert Phone Number] or [Insert Email Address].**

Sincerely,

[Name of Signing Official]

[Office of Signing Official]

Appendix C. Press Release

[DATE]

FOR IMMEDIATE RELEASE

[COMPONENT NAME]

[COMPONENT LOGO]

[DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT OPENS INVESTIGATION INTO **[BRIEF DESCRIPTION OF PRIVACY]**

WASHINGTON - The Department of Housing and Urban Development announced today that it has opened an investigation into **[Type of Incident and Method of Potential Personally Identifiable Information (PII) Compromise]. [Explain circumstances of incident and involvement of third parties (e.g., package mailing companies, local police, etc)].**

The **[Insert Component or office name]** is completely committed to safeguarding PII. Investigators from **[Component Name]** will assess whether policies or procedures should be modified to prevent similar incidents from occurring and to reduce the risk to PII. In the interim, **[Component Name]** has sent letters to all persons who are potentially affected by the privacy incident, notifying them of the incident, stating that all necessary actions are being taken to protect the individuals involved, and providing instructions for redress.

Persons affected by the privacy incident may contact **[Point of Contact]** at [(_) - _____]. Media inquiries should be directed to the HUD Public Affairs Office at **[( ) -].** ###

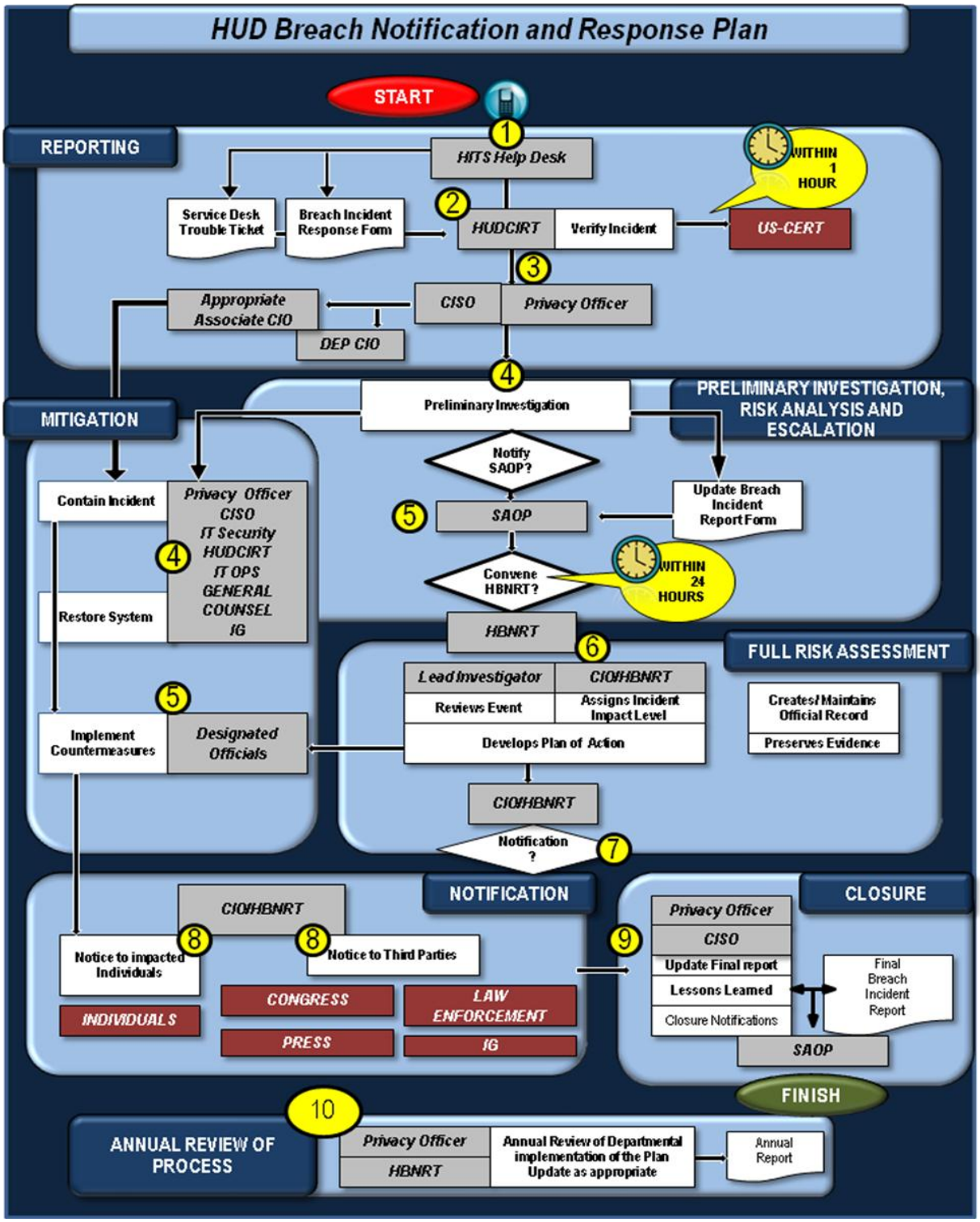
[Short Summary of Component Mission]

View this document online **[URL]**

[Component] Public Affairs

[Component Website URL]

Appendix D. Breach Notification Response Plan Process Flow



Appendix E. Roles and Responsibilities Checklists

Privacy Officer Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
Overall			
1. Reviewed the **Privacy Incident Report** to ensure: • Completeness? • Accuracy?	☐	☐	☐
2. Consulted with: • the CIO • Deputy CIO • Associate CIO for Information Assurance • CISO concerning privacy incident handling?	☐	☐	☐
3. Worked with the CISO and IT Security to contain privacy incidents: • Instructed not to print/forward email? • Instructed to physically secure under lock? • Instructed to minimize disclosure of knowledge of the potential privacy incident?	☐	☐	☐
Escalation			
4. Assessed the **preliminary privacy risk** posed by the privacy incident (e.g., low, moderate, or high impact) with the CISO.	☐	☐	☐
5. Evaluated with the CISO whether the data elements constitute the type of information that may pose a risk of identity theft?	☐	☐	☐
6. Conferred with the CISO and recommended to the SAOP whether to convene the HBNRT? • The HBNRT must be convened when the preliminary privacy risk assessment results in a High- and Moderate- privacy incidents impact level. • You and the CISO must manage Low- privacy incident impact levels.	☐	☐	☐
7. Conferred with the CISO and recommended to the SAOP who should compose the HBNRT? • The IG must be notified immediately to work closely with you and CISO when the privacy incident involves a risk of identity theft or criminal violations. • The CHO must be notified immediately to work closely with you and CISO when the privacy incident is related to HUD personnel.	☐	☐	☐
8. Confirmed **Privacy Incident Impact** Level with the consultation of the HBNRT? • 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 - impact (distress, Moderate inconvenience, or corrective action) to affected individuals - Significant corrective action possibly required by HUD	☐	☐	☐

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
• 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			
Investigation			
9. **Documented the investigation** and gathered all information necessary to describe and address the Privacy Incident Impact Level 3?	☐	☐	☐
10. Reviewed the **Privacy Incident Report** submitted to US-CERT and identified any additional information necessary?	☐	☐	☐
11. Confirmed what personal information is lost or at risk?	☐	☐	☐
12. Identified the steps taken to reduce the risk of harm?	☐	☐	☐
13. Ensured that investigators create and maintain a **chain-of-custody** log of all personnel who have access to the evidence and keep a record of: • Individuals who have touched each piece of evidence? • Date? • Time? • Locations of where the evidence is stored?	☐	☐	☐
Notification			
14. Assessed the **need** for notification by asking: • Was the incident the result of a criminal act? • Is the incident likely to result in a criminal act? • Was storage device (rather than PII itself) target of the theft? • Is there evidence that compromised information is being used to commit identity theft? • Is there substantial harm, embarrassment, inconvenience, or unfairness that could occur from this loss?	☐	☐	☐
15. Evaluated the affected **PII** for: • Accessibility? • Sensitive in combination?	☐	☐	☐
16. Assessed the privacy incident for: • Urgency? • Involvement of Law Enforcement? • Adequacy of Contact Information? • Number of Affected Individuals?	☐	☐	☐
17. Determined whether notification should be made by: • USPS? • Email? • Telephone? • Government-provided services? • Public media? • HUD website?	☐	☐	☐
18 In consultation with the CISO, recommended to the HBNRT how and when to provide notification to affected individuals?	☐	☐	☐

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
Notification Content			
19. Included a brief description, including date(s) of the breach and of its discover?	☐	☐	☐
20 Identified the types of **PII** and related information involved?	☐	☐	☐
21. Stated 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?	☐	☐	☐
22. Described the steps individuals should take **to protect themselves** from potential harm?	☐	☐	☐
23. Informed the individual of the **steps the Department has underway** to investigate the breach, to mitigate losses, and to protect against any further breaches?	☐	☐	☐
24. Provided the Deputy Assistant Secretary for Public Affairs as the **Point of Contact** for affected individuals to contact for more information, including a toll-free number, website, and/or postal address?	☐	☐	☐
25. Included only the type of PII and **not any specific PII** concerning affected individuals?	☐	☐	☐
26. Complied with **508 requirements**?	☐	☐	☐
27. Included a **TTY number** provided for affected individuals with visual or auditory impairments?	☐	☐	☐
28. Updated Privacy Incident Report with the SAOP's decision regarding **who** shall issue the notice?	☐	☐	☐
29. Updated the Privacy Incident Report with the notice issued?	☐	☐	☐
Mitigation			
30. Considered opportunities to **mitigate risk**, in collaboration with the CISO: • Notification of affected individuals, the public, and other government entities (e.g. Congress) pursuant to the Notification section of this document? • Removing exposed information from an Internet or Intranet page? • Notification of external law enforcement (subject to notification and concurrence by the HBNRT) in coordination with the Investigation and Notification phases? • Contacting appropriate financial institutions for incidents involving credit cards? • Offering of initial credit report, additional credit monitoring, or identity-theft monitoring services to mitigate the misuse of PII and to identify patterns of suspicious behavior? • Agency review of decisions regarding individuals, in cases where data or perspectives used to make decisions may have been compromised due to the incident?	☐	☐	☐
31. Worked with the CISO, IT Security, and the owner of the impacted system to determine the appropriate steps for restoring the integrity of the compromised technical system?	☐	☐	☐
32. Worked jointly with the Program manager of the impacted data store and with the CIO to ensure security is re-established for the affected data store for paper-based incidents?	☐	☐	☐
33. With the CISO, noted any implemented mitigation countermeasures in the Privacy Incident Report?	☐	☐	☐
Closure			
34. Made **incident closure recommendations** in consultation with the HBNRT?	☐	☐	☐

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
35. **Updated the privacy incident report** to recommend incident closure, subject to review by the CIO and the HBNRT?	☐	☐	☐
36. Followed-up with HUDCIRT to ensure all information is up to date and that HUDCIRT is in concurrence with the incident closure?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
37. Identified and posted lessons learned?			
38. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐
39. Maintained and **updated point-of-contact (POC)** information for privacy incident handling?	☐	☐	☐
40. Prepared **an annual report** for the CIO • Outlining the lessons learned from privacy incidents that occurred during the year? • Identifying ways to strengthen Departmental safeguards for PII and to improve privacy-incident handling?	☐	☐	☐

Chief Information Security Officer (CISO) Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
Overall			
1. Reviewed the **Privacy Incident Report** to ensure: • Completeness? • Accuracy?	☐	☐	☐
2. Consulted with: • the CIO • Deputy CIO • Associate CIO for Information Assurance • CISO concerning privacy incident handling?	☐	☐	☐
3. Worked with the Privacy Officer and IT Security to **contain** privacy incidents: • Instructed not to print/forward email? • Instructed to physically secure under lock? • Instructed to minimize disclosure of knowledge of the potential privacy incident?	☐	☐	☐
Escalation			
4. Assessed the **preliminary privacy risk** posed by the privacy incident (e.g., low, moderate, or high impact) with the Privacy Officer.	☐	☐	☐
5. Evaluated with the Privacy Officer whether the data elements constitute the type of information that may pose a risk of identity theft?	☐	☐	☐
6. Conferred with the Privacy Officer and recommended to the SAOP whether to convene the HBNRT? • The HBNRT must be convened when the preliminary privacy risk assessment results in a High- and Moderate- privacy incidents impact level. • You and the Privacy Officer must manage Low- privacy incident impact levels.	☐	☐	☐
7. Conferred with the Privacy Officer and recommended to the SAOP who should compose the HBNRT? • The IG must be notified immediately to work closely with you and the Privacy Officer when the privacy incident involves a risk of identity theft or criminal violations. • The CHO must be notified immediately to work closely with you and the Privacy Officer when the privacy incident is related to HUD personnel.	☐	☐	☐
8. Confirmed **Privacy Incident Impact** Level with the consultation of the HBNRT? • 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 - impact (distress, Moderate inconvenience, or corrective action) to affected individuals - Significant corrective action possibly required by HUD • Privacy Incident Impact Level 1 (High) - SPII involved	☐	☐	☐

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
- Potentially high impact (distress, inconvenience or corrective action) by affected individual(s) - Potentially adverse effect on organizational operations, assets, reputation, and affected individuals			
Investigation			
9. **Documented the investigation** and gathered all information necessary to describe and address the Privacy Incident Impact Level 3?	☐	☐	☐
10. Reviewed the **Privacy Incident Report** submitted to US-CERT and identified any additional information necessary?	☐	☐	☐
11. Confirmed what personal information is lost or at risk?	☐	☐	☐
12. Identified the steps taken to reduce the risk of harm?	☐	☐	☐
13. Ensured that investigators create and maintain a **chain-of-custody** log of all personnel who have access to the evidence and keep a record of: • Individuals who have touched each piece of evidence? • Date? • Time? • Locations of where the evidence is stored?	☐	☐	☐
Notification			
14. Made recommendations to the HBNRT **regarding the propriety of external notification** to affected third parties?	☐	☐	☐
15. Made recommendations to the HBNRT regarding the **means of external notification** to affect third parties?	☐	☐	☐
16. Made recommendations to the HBNRT regarding the propriety of the issuance of a **press release** for privacy incident impact levels moderate and high?	☐	☐	☐
17 Assessed the **need** for notification by asking: • Was the incident the result of a criminal act? • Is the incident likely to result in a criminal act? • Was storage device (rather than PII itself) target of the theft? • Is there evidence that compromised information is being used to commit identity theft? • Is there substantial harm, embarrassment, inconvenience, or unfairness that could occur from this loss?	☐	☐	☐
18. Evaluated the affected **PII** for: • Accessibility? • Sensitive in combination?	☐	☐	☐
19. Assessed the privacy incident for: • Urgency? • Involvement of Law Enforcement? • Adequacy of Contact Information? • Number of Affected Individuals?	☐	☐	☐

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
20. Determined whether notification should be made by: • USPS? • Email? • Telephone? • Government-provided services? • Public media? • HUD website?	☐	☐	☐
21. In consultation with the Privacy Officer, recommended to the HBNRT how and when to provide notification to affected individuals?	☐	☐	☐
Mitigation			
22. Considered opportunities to **mitigate risk**, in collaboration with the Privacy Officer: • Notification of affected individuals, the public, and other government entities (e.g. Congress) pursuant to the Notification section of this document? • Removing exposed information from an Internet or Intranet page? • Notification of external law enforcement (subject to notification and concurrence by the HBNRT) in coordination with the Investigation and Notification phases? • Contacting appropriate financial institutions for incidents involving credit cards? • Offering of initial credit report, additional credit monitoring, or identity-theft monitoring services to mitigate the misuse of PII and to identify patterns of suspicious behavior? • Agency review of decisions regarding individuals, in cases where data or perspectives used to make decisions may have been compromised due to the incident?	☐	☐	☐
23. Worked with the Privacy Officer, IT Security, and the owner of the impacted system to determine the appropriate steps for restoring the integrity of the compromised technical system?	☐	☐	☐
24. With the Privacy Officer, noted any implemented mitigation countermeasures in the Privacy Incident Report?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
25. Identified and posted lessons learned?	☐	☐	☐
26. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐
27. Maintained and **updated point-of-contact (POC)** information for privacy incident handling?	☐	☐	☐

Senior Agency Official for Privacy Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
Overall			
1. Served as an **advocate for privacy and computer security incident response activities** in consultation with the CISO and Privacy Officer?	☐	☐	☐
2. Advised the Secretary of any **issues arising from privacy incidents** that affect: • Issues that may cause public concern? • Issues that may cause loss of credibility?	☐	☐	☐
3. Ensured that incidents are **reported within the required reporting time requirements**?	☐	☐	☐
4. Received preliminary risk assessment from the Privacy Officer and CISO?	☐	☐	☐
5. If a moderate or high impact privacy incident is involved, reported the findings to: • COO • IG • HCO • GC • CRM • CPO • DepSec • Program Manager of the program experiencing the breach?	☐	☐	☐
6. Decided whether to convene the HBNRT?	☐	☐	☐
7. Served as chair of the HBNRT	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
8. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

Chief Information Officer Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
Overall			
1. Provided **management direction** to security operations?	☐	☐	☐
2. Served as an **advocate for privacy and computer security incident response activities** in consultation with the CISO and Privacy Officer?	☐	☐	☐
3. Advised the Secretary of any **issues arising from privacy incidents** that affect: • Infrastructure protection? • Vulnerabilities?	☐	☐	☐
Individual Notification			
4. Decided **whether** notification is necessary?	☐	☐	☐
5. Decided **who** should issue the notification, if not the HUD Secretary?	☐	☐	☐
6. Decided **how and when** notification should be provided?	☐	☐	☐
7. Approved the **content** of the notification?	☐	☐	☐
Third Party Notification			
8. Determined the need to notify external third parties (beyond affected individuals)?	☐	☐	☐
9. Confirmed if there any criminal violations relating to the disclosure or use of PII and Covered Information? If yes, have you verified that the IG promptly notified 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?	☐	☐	☐
10. Determined if the privacy incident requires communications with members of Congress and their staffs? • If yes, have you verified that the HBNRT notified the Assistant Secretary for Congressional and Intergovernmental Relations immediately?	☐	☐	☐
11. Determined if the privacy incident involves government-authorized credit cards or individuals' bank account numbers that are used in employment-related transactions (e.g., payroll)? • If yes, have you verified that the CFO in consultation with the HBNRT promptly notified the bank or other entity that is responsible for the particular transaction?	☐	☐	☐
12. Determined if the privacy incident mitigation or notification processes require communication with or through the press? • If yes, have you verified that the General Deputy Assistant Secretary for Public Affairs, in coordination with the HBNRT, has directed all meetings and discussion with the news media and public?	☐	☐	☐
Pre-Notification Internal Coordination			
13. Coordinated notification with HUD Senior Officials?	☐	☐	☐
14. Coordinated notification with HUD Public Affairs?	☐	☐	☐
15. Coordinated notification with HUD Legislative Affairs?	☐	☐	☐
Mitigation/Closure			
16. Planned and led the activities required to resume the regular operations of the impacted Program?	☐	☐	☐

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
17. Advised the Secretary of any **issues arising from privacy incidents** that affect: • Infrastructure protection? • Vulnerabilities?	☐	☐	☐
18. Worked jointly with the Program manager of the impacted data store and with the Privacy Officer to ensure security is re-established for the affected data store for paper-based incidents?	☐	☐	☐
19. Accepted the Privacy Officer's recommendation to close the incident?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
20. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

Chief Financial Officer Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. Served on the HBNRT when **CFO designated financial systems** are involved in the privacy incident?	☐	☐	☐
Investigation			
2. Collaborated with IG, if identity theft is implicated?	☐	☐	☐
3. Provided documentation of CFO-related information for the Privacy Incident Report, as necessary?	☐	☐	☐
Notification			
4. **Notified** the issuing bank where the privacy incident involves government-authorized credit cards, in consultation with the HBNRT?	☐	☐	☐
5. **Notified the bank or other entity** involved where 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, after consultation with the HBNRT?	☐	☐	☐
6. **Recommended** to the Chair of the HBRNT in consultation with other members of HBNRT regarding • The propriety of external notification to affected third parties? • The issuance of a press	☐	☐	☐
Mitigation			
7. Approved **reimbursement** of expenses related to investigation of privacy incidents?	☐	☐	☐
8. Collaborated with Chief Procurement Officer for the order of any **credit monitoring services**?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
9. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

Chief Procurement Officer Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. Been notified by the HBNRT that **credit monitoring services are necessary** for a particular suspected or confirmed privacy incident?	☐	☐	☐
2. **Reviewed the pricing and terms and conditions** of the GSA BPAs, in addition to any other credit monitoring services that the HBNRT may be considering?	☐	☐	☐
3. Determined the need to **order credit monitoring** through GSA at hourly rates as established by the FABS Schedule contracts? (The applicable services shall be Special Item Numbers (SIN) 520 16 Business Information Services.) See OMB M-07-04 *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)* December 22, 2006.	☐	☐	☐
4. **Collaborated with the CFO** to ensure funds available to procure credit monitoring services?	☐	☐	☐
GSA BPA Orders			
5. Submitted a GSA BPA with: • Statement of Work? • Request for Quotation (RFQ) procedures? • Evaluation of the RFQs? • Documentation? • The BPA-holders considered, noting the BPA-holder from which the service was purchase • A description of the service purchased • The amount paid • The evaluation methodology used in selecting the BPA-holder to receive the task order • The rationale for any tradeoffs in making the selection • The price reasonableness determination • The rationale for using	☐	☐	☐
Alternative Credit Monitoring Services Orders			
6. Sent order of Alternative Credit Monitoring Services to: • GSA? • A copy to the OMB E-Government Administrator?	☐	☐	☐
7. Ensured the order of Alternative Credit Monitoring Services explains how the proposed contract offers a better value to the agency by: • Identify the pricing? • Identify the terms and conditions?	☐	☐	☐
8. Prepared the order of Alternative Credit Monitoring Services **in coordination with HUD's Office of the Chief Acquisition Officer and the Office of the Chief Information Officer?**	☐	☐	☐
9. Submitted the order of Alternative Credit Monitoring Services **at least 10 days** prior to making an award, except in the event of unusual and compelling urgency, in which case the notice shall be provided as soon as practicable?	☐	☐	☐

General Counsel Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. Provided **legal advice** to the HBNRT for a specific privacy incident regarding HUD personnel and the potential for: • Disciplinary action? • Corrective action?	☐	☐	☐
2. **Recommended** to the CISO and Privacy Officer in consultation with other members of the HBNRT regarding: • Propriety of external notification to affected third parties? • Issuance of a press release?	☐	☐	☐
3. Advised on whether **referral of a privacy incident** to other authorities is warranted.	☐	☐	☐
4. Served 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?	☐	☐	☐
5. Reviewed, revised, and commented on: • Reports? • Corrective actions taken?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
6. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

Inspector General Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. **Consulted** on a case-by-case basis to determine the appropriate incident handling procedures for Moderate- and High-Impact privacy incidents as warranted with: • CISO? • Privacy Officer?	☐	☐	☐
2. **Recommended** to the CISO and Privacy Officer in consultation with other members of the HBNRT regarding: • Propriety of external notification to affected third parties? • Issuance of a press release?	☐	☐	☐
3. Consulted 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.	☐	☐	☐
4. Served 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?	☐	☐	☐
Incident Investigation			
5. Was the breach **intentional**?	☐	☐	☐
6. Was employee **misconduct** involved?	☐	☐	☐
7. Was the breach was a single incident or part of a **broad-based criminal effort**?	☐	☐	☐
8. Is the incident a part of an **ongoing investigation** by the Federal Bureau of Investigation, Secret Service, or other federal, state, or local law enforcement?	☐	☐	☐
9. Would notice to individuals or third parties would **compromise an ongoing law enforcement investigation**?	☐	☐	☐
Notification			
10. Referred incidents involving potential employee involvement in breach incidents (i.e., employee misconduct) to the **Office of the Inspector General Special Investigations Division**, which is authorized to conduct employee misconduct investigations?	☐	☐	☐
11. **Notified 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?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
12. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

Program Manager Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. **Contacted the HUD Help Desk** when a privacy incident occurs?	☐	☐	☐
2. **Received initial reports** from HUD personnel regarding the possible detection of privacy incidents?	☐	☐	☐
3. **Consulted with the Privacy Officer** when necessary to obtain guidance concerning privacy incident handling and other privacy issues affecting information systems?	☐	☐	☐
4. Determined whether a **suspected or confirmed incident** involving PII may have occurred?	☐	☐	☐
5. Assisted the CISO and Privacy Officer with the **development of facts** for the Privacy Incident Report?	☐	☐	☐
6. Assisted with the **investigation and mitigation** of a privacy incident to the extent necessary?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
7. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

HUD Personnel Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. **Contacted the HUD Help Desk** when a privacy incident occurs?	☐	☐	☐
2. **Contacted your Program Manager or other HUD supervisor** regarding the possible detection of privacy incidents?	☐	☐	☐
Incident Containment			
3. Protected PII in **electronic form,** e.g. email or collaboration site, by: • Not forwarding the email? • Not deleting the PII? • Not printing the PII?	☐	☐	☐
4. Protected PII in **physical form**, e.g. mobile device, paper, by: • Placing PII under lock and key?	☐	☐	☐
5. **Refrained** from discussing the potential incident with individuals lacking a "need to know"?	☐	☐	☐
6. Assisted the CISO and Privacy Officer with the **development of facts** for the Privacy Incident Report?	☐	☐	☐
7. Assisted with the **investigation and mitigation** of a privacy incident to the extent necessary?	☐	☐	☐

Customer Relationship Manager Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. **Consulted** on a case-by-case basis to determine the appropriate incident handling procedures for Moderate- and High-Impact privacy incidents as warranted with: • CISO? • Privacy Officer?	☐	☐	☐
2. **Reviewed** contracts related to effected vendors for: • Security obligations? • Responsibilities for mitigation costs? • Proper roles and responsibilities? • Accountability procedures?	☐	☐	☐

3. **Recommended** to the CISO and Privacy Officer in consultation with other members of the HBNRT regarding:
• Propriety of external notification to affected third parties?
  • Communication with the public?
  • Communication with affected individuals?
  • Communication with affected vendors?
• Issuance of a press release?
	☐	☐	☐

4. **Consulted** with the Privacy Officer in developing communication with affected/implicated vendors regarding: • Obligations to protect PII? • Obligation to participate in incident investigation, containment, and mitigation?	☐	☐	☐
5. Confirmed the press release: • Is 508-compliant? • Includes a TTY line to contact for further information? • Translated into appropriate languages? • Added to the relevant HUD website?	☐	☐	☐
6. Collaborated with the CFO and other members of HBNRT regarding the issuance of a press release in privacy incidents involving **CFO-designated financial systems**?	☐	☐	☐
7. Confirmed notice is appropriate **after consulting IG and GC regarding law enforcement investigations**?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
8. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

General Deputy Assistant Secretary for Public Affairs Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. **Consulted** on a case-by-case basis to determine the appropriate incident handling procedures for Moderate- and High-Impact privacy incidents as warranted with: • CISO? • Privacy Officer?	☐	☐	☐

2. **Recommended** to the CISO and Privacy Officer in consultation with other members of the HBNRT regarding:
• Propriety of external notification to affected third parties?
  • Communication with the public?
  • Communication with affected individuals?
• Issuance of a press release?
	☐	☐	☐

3. Coordinated with HBNRT regarding the **appropriateness and timing** of a press release with the notification of third parties? For example, • If criminal violations are involved, untimely press releases may compromise the investigation • If government-authorized credit cards used in employment-related transactions (e.g., payroll) that include individuals' bank account numbers are involved, press releases may compromise the mitigation strategies	☐	☐	☐
4. Confirmed a press release is appropriate after consulting **IG and GC regarding incidents with potential criminal violations**?	☐	☐	☐
5. Collaborated with the CFO and other members of HBNRT regarding the issuance of a press release in privacy incidents involving **CFO-designated financial systems**?	☐	☐	☐
6. Led all meetings and discussion with the news media and public, if mitigation or notification processes required communication with or through the press?	☐	☐	☐
7. Collaborated with the Privacy Officer to ensure that the **press release contains all relevant information** describing the privacy incident? The information could 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. • Provided the Deputy Assistant Secretary for Public Affairs as the Point of Contact for affected individuals to contact for more information, including a toll-free number, website, and/or postal address?	☐	☐	☐
8. Ensured the press release is: • 508-compliant? • Translated into appropriate languages? • Posted to the relevant HUD (and other) websites?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
9. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

Human Capital Officer Roles and Responsibilities Checklist

Breach Management			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
1. Coordinated with the **General Counsel and the HBNRT** for a specific privacy incident regarding HUD personnel and the potential for: • Disciplinary action? • Corrective action?	☐	☐	☐
2. For incidents regarding **HUD personnel**, you have reviewed, revised, and commented on: • Reports? • Corrective actions taken?	☐	☐	☐
3. Coordinated with HBNRT regarding the **appropriateness and timing** of: • Press releases? • Third party notification? • Individual notification?	☐	☐	☐
4. Collaborated with **IG and GC** regarding HUD personnel-related incidents with potential criminal violations?	☐	☐	☐
HBNRT Administration			
Have you completed the following responsibilities?	**Yes**	**No**	**N/A**
5. **Reviewed implementation of this guidance** at least annually or whenever there is a material change in HUD practices? • Date last reviewed: _____	☐	☐	☐

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*.

2. OMB M-07-16, May 22, 2007.

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.

Appendix F. Acronyms

CD	Compact Disk
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DOB	Date of Birth
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
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
Ops	Operations
PII	Personally Identifiable Information
POC	Point of Contact
SOR	System of Record
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team

Appendix G. List of References

1. U.S. Department of Housing and Urban Development Privacy Act Handbook 1325.01 REV-1.
2. U.S. Department of Housing and Urban Development Privacy Principles.
3. 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."
4. 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.
5. OMB Memorandum 06-15, *Safeguarding Personally Identifiable Infor*mation, 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.
6. OMB's Memorandum, *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.
7. 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.
8. 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.
9. 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.
10. 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.
11. *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.
12. 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.

13. 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.
14. 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.
15. 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.
16. Federal Trade Commission. (2001, January 18). *Federal Trade Commission Bureau of Consumer Protection Division of Financial Practices*. Retrieved April 30, 2010, from The Gramm-Leach Bileley Act Privacy of Consumer Financial Information: http://www.ftc.gov/privacy/glbact/glboutline.htm.
17. United States Department of Homeland Security Privacy Incident Handling Guidance Version 2.1 September 10, 2007.
18. U.S. Department of Commerce, National Institute of Standards and Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Draft NIST Special Publications (SP) 800-122 (Draft).
19. U.S. Department of Commerce, National Institute of Standards and Technology, Recommended Security Controls for Federal Organizations and Information Systems NIST Special Publications (SP) 800-53 Revision 3.
20. U.S. Government Privacy, Essential Policies and Practices for Privacy Professionals (McEwen & Shapiro, 2009).