US DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

HUD Privacy Handbook
1325.1 REV. 1.0

10/18/2021

This document contains confidential information for official use by the United States HUD only. It shall not be duplicated, used, or disclosed in whole or in part without prior written permission from the Privacy Office.

Document Change History

Issue	Date	Description
Revision 1.0	10/18/2021	Replaces Privacy Act Handbook (1325.1).

Table of Contents

1.0 Introduction

The U.S. Department of Housing and Urban Development (HUD) Privacy Handbook establishes policies, procedures, requirements, and guidelines for the implementation of HUD's Privacy responsibilities. These requirements include personally identifiable information (PII) handling policies and procedures, information disclosure and accounting, risk assessments, data use inventorying and recordkeeping, Federal reporting, and forms and contracts requirements.

1.1 Rescission

This Handbook will be titled HUD Privacy Handbook 1325.1 Rev. 1.0, which replaces and rescinds Privacy Act Handbook 1325.1.

1.2 Applicability

This Handbook applies to all HUD Personnel and contractors unless the responsibility is role-specific.

1.2.1 Privacy Liaison Officers (PLOs)

Privacy Liaison Officers (PLOs) serve as the point of contact between the Privacy Office and their respective Program Offices. This subsection outlines the main PLO responsibilities and the corresponding sections of the Handbook that provide guidance on fulfilling those responsibilities:

- Coordinating with the Privacy Office and System Owners to ensure systems within their Program Office have proper privacy documentation.
    - System of Record Notices (SORN) (Section 6.0)
    - Privacy Impact Assessments (PIA) (Section 5.0)
    - Computer Matching Agreements (CMA) (Section 7.0)
    - Proper privacy notices and Privacy Act Statements (Section 9.0)
    - Social Security Number (SSN) Justification Memos and Reduction Plans (Section 2.2.8, 2.2.9)
- Collaborating with System Owners and the Privacy Office to ensure Cyber Security Assessment and Management (CSAM) information for systems is up to date.

1.2.2 System Owners

System Owners manage HUD information systems. This subsection outlines the main System Owner privacy responsibilities and the corresponding sections of the Handbook that provide guidance on fulfilling those responsibilities:

- Coordinating with the Privacy Office and PLOs to ensure systems within their Program Office have proper privacy documentation.
    - System of Record Notices (SORN) (Section 6.0)
    - Privacy Impact Assessments (PIA) (Section 5.0)

    - Computer Matching Agreements (CMA) (Section 7.0)
    - Proper privacy notices and Privacy Act Statements (Section 9.0)
    - Social Security Number (SSN) Justification Memos and Reduction Plans (Section 2.2.8 & 2.2.9)
- Updating CSAM privacy controls inputs that apply to their systems (Section 3.0)

1.3 Effective Date

This Handbook is effective as of 10/18/2021.

2.0 Personally Identifiable Information (PII) Handling Policies and Procedures

2.1 Definition of PII

Per the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Set forth below is a non-exclusive list of information that may constitute PII on its own or in combination with other information:

- Age
- Alias
- Audio recordings
- Biometric identifiers (e.g., fingerprints, iris image)
- Certificates (e.g., birth, death, marriage)
- Credit card number
- Criminal records information
- Date of birth
- Device identifiers (e.g., mobile devices)
- Drivers' License / State ID Number
- Education Records
- Email address
- Employee identification number
- Employment status, history, or information (e.g., title, position)
- Fax number
- Financial information
- Foreign activities
- Full name
- Gender
- Geolocation information
- Home address
- Internet cookies containing PII
- Investigation report or database
- IP / MAC address
- Legal documents or records
- Marital status
- Military status or other information
- Mother's maiden name
- Passport information
- Phone numbers
- Photographic identifiers
- Place of birth
- Protected health information
- Race/ethnicity
- Religion
- Salary
- Sex
- Social security number (SSN)
- Taxpayer ID
- User ID
- Vehicle identifiers
- Web uniform resource locators
- Work address or other business contact information. (HUD does not engage with individuals in an entrepreneurial capacity, but business contact information may still constitute PII because it identifies individuals.)

2.2 Privacy Policy

The HUD Privacy Policy establishes the Department's rules and protocols for complying with Federal Privacy requirements.

2.2.1 Exclusions

The HUD Privacy Policy pertains to HUD's collection and handling of personal information. HUD follows certain exceptions outlined in the Privacy Act of 1974. (See Section 4.6 of this Handbook for details). Other exceptions to this policy are expected to be requested only in unusual or exceptional circumstances; these must be documented by relevant stakeholders and then approved by HUD's Senior Agency Official for Privacy (SAOP).

2.2.2 Responsibility

a. **All HUD personnel** handling PII must comply with PII handling requirements outlined in the Privacy Policy. Noncompliance will result in reports to the PLO and possible escalation to the Privacy Office.
    i **Office Managers** are responsible for ensuring personnel understand the terms of the Privacy Policy and the penalties for noncompliance.
    ii **Office Managers** must notify PLOs of any Privacy Policy violations and noncompliance.
b. As delegated by the **SAOP**, the **Chief Privacy Officer (CPO)** has executive oversight and is responsible for the implementation of the HUD Privacy Policy.
c. **PLOs** are responsible for tracking violations of the Privacy Policy and reporting them to the Privacy Office.

2.2.3 PII Handling

Per the NIST SP 800-122, which provides government-wide standards for protection of agency PII, HUD requires strict PII handling guidelines for employees and contractors due to the nature of the data collected and used by HUD, and the increased risk to an individual if sensitive or personal data were to be compromised.

a. General Handling

Methods for handling PII include but are not limited to the below. They must be conducted in accordance with HUD's approved records schedules and system of records notice (SORN), as applicable.

- Store PII on secure HUD network, systems, and HUD-approved media;
- Secure paper PII data by locking it in desks and filing cabinets;
- Remove visible PII from desks and office spaces when not in use (e.g., at the end of each day);
- Destroy PII by shredding;
- Delete electronic PII by emptying computer "recycle bin";
- Only use HUD-provided email addresses for conducting official business; and
- Encrypt PII on computers, media, and other devices, especially when

sending data outside of HUD's network.

b. Distribution and Transmission

PII may be distributed or released to other individuals only if: (1) it is within the scope of the recipient's official duties; (2) the recipient has an official, role-based need to know; and (3) sharing information is done in a secure manner. When in doubt HUD personnel must treat PII as sensitive and must keep the transmission of PII to a minimum, even when it is protected by secure means.

Ways for communicating, sending, and receiving PII include:

- Secure File Transfer Protocol (FTP) – Files may be uploaded to HUD systems through an approved secure FTP.
- Facsimile – When faxing information, HUD personnel should include an advisory statement about the contents on the cover sheet and should notify the recipient before and after transmission.
- Verify that the recipient knows the fax will be transmitted so that the information does not sit at the fax machine unattended.
- Mail – HUD personnel should physically secure PII when in transit by sealing it in an opaque envelope or container, and mail it using First Class or Priority Mail, or a comparable commercial service. HUD personnel should not mail, or send by courier PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.
- Email – When emailing PII within HUD or outside of HUD, secure the PII by encrypting it. Never email PII other than your own to personal email accounts or devices.
- Hard Copy – HUD personnel should hand-deliver documents containing PII whenever needed and as feasible. HUD personnel should not leave PII unattended on printers, facsimile machines, copiers, or in other common places. When delivering hard copy documents, personnel should use the PII Coversheet to enclose all materials containing PII. For details regarding physical PII Handling, see the PII Protection at Workstations Policy.

2.2.4 PII Processing Requirements

The following principles apply to the processing of PII. These principles are based on the Fair Information Practice Principles (FIPPs) and are mirrored in Federal privacy legislation as well as OMB requirements.

a. Access and Amendment:

HUD should provide individuals with appropriate access to their own PII and the opportunity to correct or amend that PII.

b. Accountability:
HUD should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. HUD should also clearly define the roles and responsibilities with respect to PII for all employees and contractors and should provide appropriate training to all employees and contractors who have access to PII.

The Privacy Office is responsible for ensuring privacy awareness training is provided to all contractor and third party personnel as well as ensuring role-based privacy training is provided to all personnel with privacy responsibilities.

c. Authority:
HUD should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate documentation.

d. Minimization:
HUD should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

Where feasible and within the limits of technology, HUD should locate and remove/redact specified PII and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

HUD's Privacy Office maintains an inventory of PII holdings and uses the privacy impact assessment (PIA) and SORN processes to identify methods to further reduce the data the Department collects and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Records containing PII must be maintained in accordance with National Archives and Records Administration (NARA) and HUD-approved retention, disposition, and destruction schedules to further support the goals of privacy and security.

HUD should not collect Social Security Numbers (SSNs) unless it is both necessary and authorized. Any forms used to collect SSNs should include a Social Security Number Justification Memo explaining why collection of SSNs is necessary and which authorities permit the collection. See Section 2.2.5 of this Handbook for further details.

e. Quality and Integrity:
HUD should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

f. Individual participation:
HUD should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. HUD should also establish and maintain procedures to receive and address individuals' privacy-related complaints and inquiries.

g. Purpose Specification and Use Limitation:
HUD should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

h. Security
HUD should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

i. Transparency:
HUD should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

j. Federal Record Rights
In accordance with Federal requirements, HUD should provide notice describing the individual data subject's rights in relation to personal data as follows:

- The individual data subject has access to the personal data held by HUD about them.
- The individual data subject can correct a record that is inaccurate, irrelevant, or incomplete.

Additionally, HUD should provide public access to information and instructions regarding the process and contacts for making a request to correct any record pertaining to the individual. See 4.0 of this Handbook for further guidance regarding Privacy Act requests.

k. System of Records Notice
A System of Records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. HUD adheres to the Privacy Act requirements for publishing notices of its systems of records in the Federal Register, which are referred to as SORNs.

Each SORN describes what, why, and how HUD collects, maintains, uses, and disseminates records in the system. Some systems maintain information on HUD employees while others maintain information from or about individuals outside of HUD. There are also Government-wide systems that are maintained by other Federal agencies and hold the operating authority over the records such as the Office of Personnel Management's (OPM) Employee Performance File system.

l. Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is collected, maintained, stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks. A PIA is required for each HUD information system, General Support System (GSS), or electronic collection that collects, maintains, uses, and/or disseminates PII about US citizens, Federal employees, and HUD contractors. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to the system.

2.2.5 Social Security Number Policy

This section of the Handbook establishes policy and assigns responsibilities for SSN use, reduction, and justification pursuant to the Privacy Act and OMB Memorandum 17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information.” Given the sensitive nature of SSNs, Federal requirements do not allow for collection and use of SSNs unless necessary. HUD must inventory the SSNs it does collect along with documented justification for each case where SSNs are collected and or used.

2.2.6 SSN Inventory, Authorization, and Elimination

a. SSN Inventory

The HUD Privacy Office will maintain an inventory of all systems which collect SSNs. System Owners and PLOs should complete the SSN Justification Memo and coordinate with the Privacy Office to ensure that the SSN inventory is accurate and up to date.

b. Unauthorized Collection

All HUD personnel shall reduce or eliminate the use of SSNs wherever possible. **Unless collection is allowed by a proper authority, such as Federal or state legislation, executive order, or OMB issuance, SSNs must not be collected, used or stored.** Further information regarding acceptable uses of SSNs and authorities that justify SSN use are detailed in Section 2.2.7 of this Handbook.

If a system is **not authorized by a proper authority to store SSNs**, then the **System Owner must immediately notify their PLO and the Privacy Office** to coordinate removal of SSNs.

c. Authorized Collection

Even if SSNs are authorized by a proper authority, System Owners must explore alternative identifiers that could be used instead of SSNs. Future collection and storage of SSNs is only allowed if absolutely necessary for a program function.

What Constitutes Collection?

Collection includes any request for individuals to provide or submit their SSNs in any form, whether it be digital, hard copy, or verbal. Examples of collection include but are not limited to:

- Prompting individuals to provide SSNs on any kind of form, such as web portals, surveys, benefits applications, etc.
- Providing the option to enter an SSN, even if individuals are not required to provide an SSN.
- Asking an individual to provide SSNs over the phone.
- Collection of SSN in any form, includes but is not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs.

2.2.7 Acceptable Uses of SSNs

Only the following list of uses are acceptable for ongoing use and storage of SSNs. Even if a statutory or executive authority technically allows for collection of SSNs, SSNs cannot be used at HUD unless necessary for one of the purposes specified in this subsection.

a. Security Clearance Investigation or Verification of Identity

This use case is linked to other Federal agencies that continue to use the SSN as a primary identifier. SSN may be used to verify the identity of applicants for program functions. The initiation, conducting, adjudication, verification, quality assurance, and billing fund control of background investigations and security clearances requires the use of the SSN. The SSN is the single identifier that links all aspects of these investigations together.

b. Interactions with Financial Institutions

Financial institutions may require individuals provide their SSN to open accounts. It may therefore be required to provide the SSN for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions.

c. Confirmation of Employment Eligibility

Any system that deals with employment eligibility may contain SSNs for verification of eligibility purposes, as all persons employed with United States government must provide an SSN or comparable identifier to prove that they are eligible to work.

d. Administration of Federal Worker's Compensation
Any system that deals with employment eligibility may contain the SSNs for administration of Federal worker's compensation purposes, as SSNs are used for verifying identity work eligibility.

e. Federal Tax-Payer Identification Number
The application of Federal and State income tax programs relies on the use of the SSN. As such, systems that have any function that pertains to the collection, payment, or record keeping of this use case may contain SSNs, including collections from persons doing business with HUD as defined by the Debt Collectin Act of 1986, as amended. Additionally, individuals who operate corporate entities under their own name may use their SSN as the tax number for that business function.

f. Computer Matching Systems
Systems, processes, or forms that interact with other government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to a different primary identifier that is not SSN. This case use includes collections of SSNs needed to verify eligibility for HUD's programs.

g. Research
SSNs may be used for research, data analysis, and data matching purposes.

2.2.8 SSN Justification Memo

This section provides guidance for completing and submitting the SSN Justification Memo. System Owners and PLOs should coordinate to complete and submit the SSN Justification Memo Template for any form or system that collects or stores SSNs. The SSN Justification Memo will be used to determine whether the identified uses are acceptable and compliant with Federal requirements. **SSN Justification Memos must be signed by the Program Manager and the relevant PLOs.**

2.2.9 Legacy System Migration Plan

Systems, processes, or forms that do not meet the acceptable use criteria in Section 2.2.7 of this Handbook for the continued use of the SSN may not be able to transition to another identifier in a timely manner due to an interface with a legacy system still using the SSN, or due to the excessive cost associated with the change. In these cases, the continued use of the SSN may be acceptable for a specified period of time, provided that **formalized, documented plans are in place for migration away from the SSN.**

System Owners and PLOs are responsible for coordinating with the Privacy Office to establish a plan of action and milestones (POA&M) to migrate away from SSN use. Plans to alter these use cases must consider interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that transfer away from the SSN does not cause unacceptably long interruptions to continued operations.

2.2.10 SSN Collection Forms

a. SSN Form Approval

Forms used to collect SSN must be submitted to the Privacy Office for approval and record-keeping. Forms that collect SSN should be submitted with an SSN Justification Memo, as explained in Section 2.2.8 of this Handbook.

Forms used to collect SSN must include an appropriate Privacy Advisory Statement. See Section 9.2 of this Handbook for details regarding the content and format of Privacy Advisory Statements.

b. SSN Form Review

Reviews of forms and systems that collect SSNs shall be conducted annually to verify whether SSNs continue to be necessary. If SSNs are no longer necessary, the System Owner should coordinate with their Program Lead, PLO(s) and the Privacy Office to remove SSNs.

2.2.11 PII Protection at Workstations Policy

The HUD PII Protection at Workstations Policy covers the responsibilities of personnel regarding the protection of information assets when unattended in the personal workspace. Physical protections and security measures are needed to prevent unauthorized access and disclosure of PII, in accordance with the HUD's privacy responsibilities. A printable version of the PII Protection at Workstations Policy is available on the HUD Privacy Website.

3.0 Privacy Controls and Controls Assessment

HUD implements the NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5 (NIST SP 800-53, Rev. 5) guidance for selecting appropriate controls and safeguarding measures for PII. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. NIST provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form.

This section of the Handbook describes responsibilities for both maintenance and implementation of privacy controls.

3.1 Privacy Controls Inheritability

Privacy controls are often closely related and function in tandem with cybersecurity controls. Controls Implementation statements are descriptions for how the department applies and fulfills NIST-established controls. **Privacy controls are implemented on both the organization-wide level and on the individual system-level**.
Organization-level controls are fulfilled and assessed at the Department level, meaning System Owners can "inherit" these controls and sub-controls.
System-level controls are privacy controls that are implemented on the individual systems.
Hybrid controls are controls that have some components implemented at the organization level and other components which are implemented on the system level.

For example, proper risk assessment control implementation requires both the policy mandating the control (organization-level) and the system owners complying with the policy by submitting necessary documentation to the Privacy Office for review (system-level).

3.1.2 Organization-Level Privacy Controls

The **Privacy Office** is responsible for updating and maintaining the implementation statements for privacy controls that are **created and maintained at the organization level**, such as privacy policies, privacy program governance, and federal reporting. Organization-wide controls are created and maintained at the Department level.

When completing implementation statements for privacy controls, **System Owners** must inherit these controls.

3.1.3 System-Level Privacy Controls

System Owners are responsible for completing implementation statements for system-level privacy controls, as these controls are maintained individually for systems.

3.1.4 Hybrid Privacy Controls

The **Privacy Office** is responsible for completing implementation statements for the organization-level components of controls which have both organization and system-level controls.

System Owners are responsible for listing the organization-level controls as inherited and for completing all system-level portions of hybrid controls.

4.0 Privacy Act Requests

This section of the Handbook sets forth procedures for processing requests for access to or amendment of records under the Privacy Act. It also includes procedures for disclosing records, and accounting for such disclosures.

Privacy Act requests can be sent to:

> Privacy Act Officer
> Department Of Housing and Urban Development
> 451 7th St. SW, Room 10139
> Washington, DC 20410

See HUD's Privacy Act webpage for more information regarding how to send a Privacy Act request.

HUD follows its Freedom of Information Act (FOIA) Office process for Privacy Act requests. Upon receiving a request, a HUD FOIA specialist determines whether the request is related to PII and or the Privacy Act. FOIA requests are processed under the FOIA (b)(6) exemption. If a matter is covered by the Privacy Act, it is forwarded to the Privacy Officer instead of being processed under the FOIA (b)(6) exemption.

FOIA specialists record the request and share the request with the relevant Program Office(s), who then have up to 10 days to deliver the necessary information back. From there, the assigned FOIA specialist analyzes the information to determine whether any PII would be included in the release or whether the request has any Privacy Act implications, and then determines the next steps for the request. These may include granting the request, making redactions to the request, or sending the request to the HUD Privacy Office.

4.1 Identity Verification

Individuals must verify their identity when making a Privacy Act access or amendment request. Pursuant to OMB M-21-04 (November 12, 2020), HUD established a process for individuals to verify their identity online by emailing a completed and signed copy of the Verification of Identity letter and two forms of identification to FOIAExecSec@hud.gov.

Forms of Identification

The following forms of identification are needed to verify individuals making Privacy Act requests. Requesting individuals must provide one form of identification from List A and another form of identification from List B below.

List A:	List B:
Driver's license	Lease or proof of residence
U.S. Passport	Utility bill
Permanent Resident Card	Insurance letter
Other state issued ID	

The FOIA Office coordinates with the Privacy Office to ensure that the Privacy Act webpage includes up to date information regarding the process and forms needed to verify identity for Privacy Act requests.

4.2 Record Amendments and Appeals

If an individual requests amendment to a record, then the Program Office in charge of the record will determine if the request is appropriate.

Within 10 business days, the Program Office should either amend the record or refuse to amend. If the Program Office refuses to amend a record, then the Program Office should notify the FOIA Office why it cannot amend the record.

The FOIA Office should notify the requesting individual why their request was denied and provide the reason the Program Office could not amend the record. The FOIA Office must also notify the individual that they have the right to appeal the decision.

4.2.1 Appeals Process

Individuals who wish to file an appeal should be directed to contact the Office of Ethics and Appeals Law Division within the Office of General Counsel (OGC). Individuals can appeal online by emailing HUDFOIAappeals@hud.gov.

The FOIA Office must provide the requesting individual with the following information when notifying the individual of their right to appeal the refusal to amend the record.

> [Name of Privacy Appeals Officer] [Title]
> Office of Ethics and Appeals Law Division
> Office of General Counsel
> U.S. Department of Housing and Urban Development
> 451 7th St., SW, Suite 2130
> Washington, DC 20410
> Telephone: (202) 708-3815
> Email: HUDFOIAappeals@hud.gov

4.3 Amendment and Amendment Refusal Process

If the individual requested an amendment to a record, the FOIA Office should log the request and any appeals or determinations made regarding the request**. The following information must be included with the record if the record is disclosed in the future**:

a. A copy of the individual's **amendment request**.
b. If the Program Office **makes the amendment**, include:
    i The date the **record was amended.**
c. If the Program Office in charge of the record **refuses to amend**:
    i Include the **date of refusal**,
    ii The **reason for not amending** the record within the **Record of Justification**.
d. If the individual **appeals the refusal to amend**:
    i Include a **copy of the individual's Statement of Disagreement**, which explains why the individual believes the record should be amended.
    ii Include a **Notice of Dispute** that identifies the portions of the record which have been disputed.

4.4 Disclosure Recordkeeping Policy

The **FOIA Office** is responsible for maintaining an accurate record of all disclosures made from any System of Records in the Privacy SharePoint, except disclosures to HUD personnel for use in the performance in their official duties or under FOIA.

Contents & Method of Disclosure Accounting
At a minimum, the disclosure accounting should contain:

- The date of the disclosure.
- A description of the information released.
- The purpose of the disclosure.
- The name and address of the person or agency to whom the disclosure was made.

Program Office Records Management Liaison Officers (RMLO) should follow FOIA's existing records management procedures for Privacy Act Requests and provide necessary information for accurate disclosure and amendment records.

If disclosure accountings are not maintained with the record and the individual requests access to the accounting, the **FOIA Office** and the **RMLO** are to **prepare a listing of all disclosures and provide this to the individual upon request**. See guidance below for detailed steps regarding procedures for disclosures, corrections and amendments, and accounting.

4.5 Disclosure Request Processing and Recordkeeping Guidance

The following provides detailed steps and additional guidance for processing requests and managing disclosure accounting.

1) **If an individual requests access to a record that is kept about them, then the individual should be allowed to:**
   a) View and review the record, unless a Privacy Act exemption applies.
   b) Bring one person of their choice to accompany them when reviewing the record.
      i) If the requesting individual brings a person with them, the requesting individual must sign a written statement authorizing that the person accompanying them will be present during any discussion or viewing of the record.
   c) Make copies of the entire record or a portion of the record.

2) **If an individual request to correct or amend a record kept about them, then the Program Office in charge of the record should:**
   a) Within 10 business days:
      i) Make the correction or amendment.
      ii) Or inform the FOIA Office that the Program Office refuses to amend the record.
         (1) **If the Program Office refuses**, it should inform the FOIA Office of the reason for refusal. The **FOIA Office** must notify the individual of:
            (a) The reason why it was refused.
            (b) The departmental procedures for how the individual can request a review of the refusal.
            (c) Provide the name and business address of the Privacy Appeals Officer who reviewed the decisions.
   b) If the individual wants the decision of refusal to amend to be reviewed, then the FOIA Office should:
      i) Review the decision **within 30 business days** of when the individual submits the request for review.
      ii) The FOIA Office **can extend the 30-day period** if there is a showing of good cause.
      iii) Upon reviewing the appeal, The FOIA Office should either affirm the decision of refusal or amend the record.

3) **If the Program Office refuses to amend the record, then:**
   a) The individual is:
      i) Permitted to file a **Statement of Disagreement** with the Department that details the reason why the individual believes they should have been allowed to amend the record.
   b) The FOIA Office should:
      i) Create a **Notice of Dispute** that identifies the portions of the record which have been disputed, and
      ii) Notify the individual of the provisions for judicial review of the HUD's refusal

to amend or correct the record.

c) Include the following documents with the record if the record is ever disclosed to other persons or agencies:
   i) Individual's **Statement of Disagreement**,
   ii) Department's **reason** for refusal, and
   iii) **Notice of Dispute**.

4.6 Privacy Act Exceptions to Conditions of Disclosure

The Privacy Act prohibits agencies from disclosing information about an individual without the individual's written consent, unless the disclosure is pursuant to one of the 12 statutory exceptions. The 12 exceptions allow disclosure:

1) To those officers and employees of the Department, who have a need for the record in the performance of their duties;
2) When disclosure is required under the Freedom of Information Act (FOIA)**;**
3) For an established routine use identified in the SORN that has been published in the Federal Register;
4) To the Census Bureau for purpose of planning or carrying out a census or survey;
5) To a recipient who has provided the Department with adequate written assurance that the record will be used solely for statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
6) To the National Archives and Records Administration (NARA) for historical preservation if the Archivist determines the record has historical value;
7) To another Department, Agency, or instrumentality of any governmental jurisdiction, within or under the control of the U.S. for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the department or instrumentality has made a written request to the HUD specifying the particular portion desired and the law enforcement activity for which the record is sought;
8) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
9) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
10) To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accountability Office;
11) Pursuant to the order of a court of competent jurisdiction;
12) To a consumer reporting agency in accordance with the Debt Collection Act.

A printable copy of these exceptions is available on the HUD Privacy Website.

4.6.1 Most Commonly Used Privacy Act Exceptions

This section highlights the exceptions that you will most likely come across in your routine responsibilities. Tips are provided below for how to handle each situation.

- Disclosures made to those officers and employees of the department which maintains the record, who have a need for the record in the performance of their duties.
    - Make sure all disclosures to officers and employees are necessary.
- Disclosures made under the Freedom of Information Act (FOIA).
    - If you are unsure if a request falls under FOIA, please contact the FOIA Office at FOIAExecSec@hud.gov.
- Disclosures made "for an established routine use identified in the SORN that has been published in the Federal Register."
    - Always check the relevant SORN.

4.7 Privacy Act Exemptions

The Privacy Act provides that HUD will provide access to records on individuals within its possession unless one of ten exemptions applies. HUD's exempted SORNs can be found at 24 Code of Federal Regulations (CFR) 16.14 and 16.15. Relevant Privacy Act exemptions for HUD include:

1) **Exemption (d)(5)** – Information compiled in reasonable anticipation of civil action or proceeding;
2) **Exemption (j)(2)** – Certain OIG systems containing records compiled in the course of a criminal law enforcement proceeding.
3) **Exemption (k)(1)** – Classified information under an Executive Order in the interest of national defense or foreign policy.
4) **Exemption (k)(2)** – Investigatory material compiled for law enforcement purposes; coverage is less broad where individual has been denied a right, privilege, or benefit as result of information sought.
5) **Exemption (k)(4)** – Information required by statute to be maintained and used solely as statistical records.
6) **Exemption (k)(5)** – Investigatory material used only to determine suitability, eligibility, or qualifications for Federal civilian employment or access to classified information when the material comes from confidential sources.
7) **Exemption (k)(6)** – Testing or examination material used to determine appointment or promotion of Federal employees when disclosure would compromise the objectivity or fairness of the process.
8) **Exemption (k)(7)** – Military evaluative records.

Most systems will not require an exemption. However, if you think that any of the above exemptions possibly applies to a system you manage or establishing, please contact the Privacy Office at privacy@hud.gov for assistance.

5.0 Privacy Impact Assessments (PIA)

HUD is required to regularly update and maintain foundational privacy artifacts such as Privacy Impact Assessments (PIAs) to comply with the E-Government Act of 2002. PIAs analyze the privacy risks as well as the protection and the process of handling information to mitigate privacy risks. Program Offices are required to complete a PIA for each HUD information system, General Support System (GSS), or electronic collection that collects, maintains, uses, and/or disseminates personally identifiable information (PII) about US citizens, Federal employees, and contractors. PIAs are also required when a new collection of information is initiated.

5.1 PIA Template and Reference Guide

The HUD PIA template and PIA Reference Guide can be found on the HUD Privacy Website. The Reference Guide provides detailed instructions and language examples for completing SORNs. **Please refer to the HUD PIA Reference Guide for a detailed, step-by-step guide for properly completing PIAs.**

5.2 What Is a PIA?

A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that System Owners and developers have incorporated privacy protections throughout the entire life cycle of a system.

5.3 Contents of a PIA

PIAs must analyze and describe:

a. What information is to be collected (e.g., nature and source),
b. Why the information is being collected (e.g., to determine eligibility),
c. Intended use of the information (e.g., to verify existing data),
d. With whom the information will be shared (e.g., another agency for a specified programmatic purpose),
e. What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent,
f. How the information will be secured (e.g., administrative and technological controls), and
g. Whether a System of Records is being created under the Privacy Act.

5.4 Is a PIA Required?

A PIA is **required for each HUD information system**, General Support System (GSS), or electronic collection that collects, maintains, uses, and/or disseminates personally identifiable information (PII) about US citizens, Federal employees, and contractors.

However, the type of PIA required depends on whether the system being assessed is new or existing.

5.4.1 What Type of PIA Is Required?

- Is this a new system?
    - If yes → See **"New PIA"**
    - If no → Does the existing system already have a PIA?
        - If yes → Has there been a change to the system that creates new privacy risks?
            - If yes → See **"Modified PIA"**
            - If no → No new PIA is needed
        - If no → See **"New PIA"** (All HUD systems must have a PIA. If for some reason a system is operating without a PIA, then the System Owner should reach out to their PLO immediately to complete a PIA.)

5.4.2 Types of PIAs

- **New PIA** – A New PIA is conducted before a new electronic System of Records is established.
- **Modified PIA** – A Modified PIA is conducted when there been a significant change to the system that creates new privacy risks or when a new collection of information has been initiated on the system.

5.4.3 PIAs – What Is a Significant Change?

1) **Conversions** – When converting paper-based records to electronic systems.
2) **Anonymous to Non-Anonymous** – When functions applied to existing information collection changes anonymous information into information in identifiable form.
3) **Significant System Management Changes** – When new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system. For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
4) **Significant Merging** – When agencies adopt or alter business processes so government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated: For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
5) **New Public Access** - When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed

by members of the public.

6) **Commercial Sources** – When agencies and departments systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources.
7) **New Interagency Uses** – When agencies and departments work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
8) **Internal Flow or Collection** – When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
9) **Alteration in Character of Data** – When new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

5.4.4 Establishing or Modifying a PIA

The workflow below describes the Privacy Office's PIA development and communication processes. A printable version of the workflow is available. Please use the HUD PIA Template to provide the Privacy Office with required information. For detailed instructions on how to properly fill out a PIA, please see the HUD PIA Reference Guide.

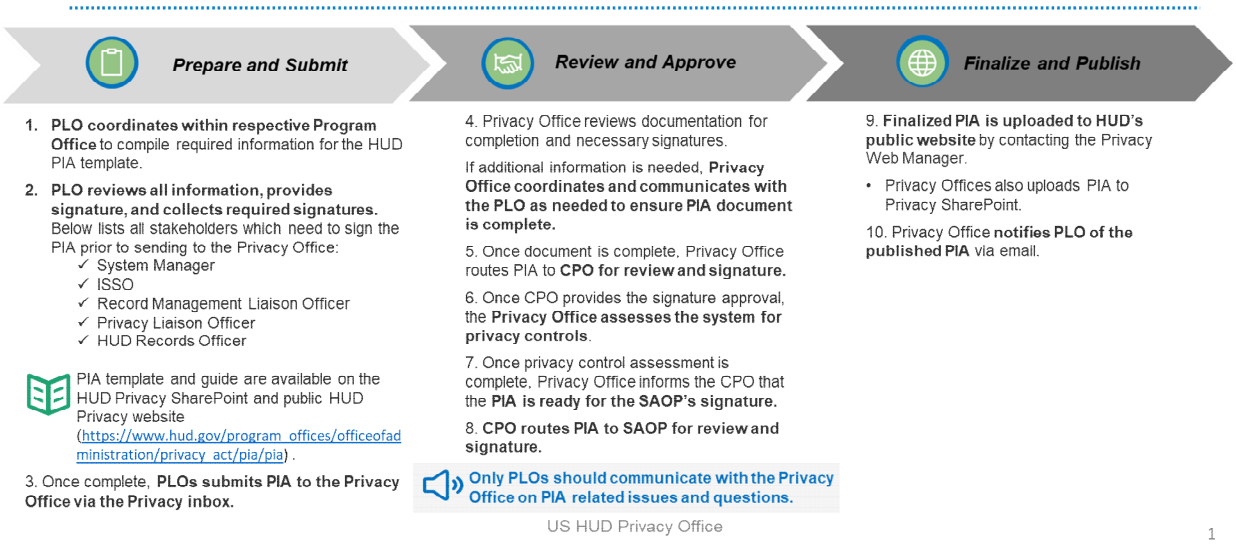

Diagram 1. PIA Workflow

5.5 PIA Review Schedule and Process

This section establishes a schedule and process for ensuring PIA reviews are conducted in a recurring and timely manner.

In addition to standard Continuous Monitoring procedures, PIAs should be reviewed not less than annually to ensure accuracy and to make note of any significant changes that may need to be reported.

5.5.1 PIA Review Schedule

Action	Timing
PLOs should initiate the **annual PIA review** and inform **System Owners** in their respective Offices to review PIAs beginning on June 1st of each year. **The first annual review for a PIA need not be conducted unless the PIA was first established at least one year prior.** • **PLOs** should begin working with **System Owners** to review PIAs to determine if **Modified PIAs** are needed. See Section 5.4 of this Handbook for details. • If **Modified PIAs** are not needed, **PLOs** should work with **System Owners** to submit **Annual PIA Certifications** to confirm PIA accuracy. See Section 5.4 of this Handbook for details and instructions. All necessary updates must be submitted to the Privacy Office by June 30th.	June 1st
PLOs should conduct a status check for which Offices have and have not submitted **Modified PIAs** and or **Annual PIA Certifications**. • **PLO**s should send submission reminders to **System Owners** who have not submitted their **Modified PIAs** and or **Annual PIA Certifications**.	Not later than (NLT) June 15th
System Owners in each Office should complete reviewing PIAs and ensure **Modified PIAs** and or **Annual PIA Certifications** are completed and submitted to the Privacy Office at privacy@hud.gov.	NLT June 30th

Table 1. PIA Review Schedule

5.5.2 Annual PIA Review Process

PLOs should work with **System Owners** to review PIAs that were first established more than one year ago (as of June 1st of the current year). If the first PIA for a system was established within one year as of June 1st of the current year, the PIA does not need to be reviewed and updated until the next year.

PLOs and **System Owners** should determine if the PIAs are up to date, or if **Modified PIAs** are needed. Refer to Section 5.4 of this Handbook to determine if a Modified PIA is needed.

Modified PIAs

- To determine if a Modified PIA is needed, refer to Section 5.4 of this Handbook for next steps.
- If a Modified PIA is needed, refer to Section 5.5 of this Handbook for next steps.

Modified SORNs

- If a system requires a Modified PIA, it will also likely require a Modified SORN, if applicable. See Section 6.5 of this Handbook for details.
- System Owners must inform Program Owners and PLOs about any system changes.
- Program Owners are responsible for coordinating with System Owners, PLOs, and the Privacy Office to ensure that the system's SORN reflects current use and program functions.

5.5.3 Annual Certifications for Existing PIAs

If no Modified PIAs are needed, Offices should make a copy of the existing PIA for the system, enter the current date, and mark the box that says, "**This is an annual certification for an existing PIA.**" Offices should submit the **Annual PIA Certifications** document to the Privacy Office.

1. Using the HUD PIA Template, insert all relevant information for the system.
2. On the very last page, check the box that says "**This is an annual certification for an existing PIA.**"
3. Insert the current date.
4. **PLOs** and **System Owners** sign the Annual PIA Certification.
5. **PLOs** submit the updated and signed Annual PIA Certification to the Privacy Office at privacy@hud.gov with the subject field, "Annual PIA Certification [Year], [Office Name]."

5.6 PIA Website Publication

The Privacy Office is responsible for posting the first page of PIAs to the HUD Privacy Website. **Only Section 1 of PIAs should be published to the website; the full PIA should be kept only for internal use as system information can be sensitive**. The Privacy Office should maintain an updated SharePoint inventory of PIAs that includes the full PIAs as well as the redacted public web versions.
Retiring PIAs

Any time a system is retired, the PIA for the respective system should be moved to the Retired PIAs section of the HUD Privacy Website.

6.0 System of Records Notices (SORN)

The Privacy Office ensures compliance with the Privacy Act of 1974 by developing and maintaining SORNs. A System of Records is a group of any records under the control of any agency or department from which information is retrieved by a unique identifier, including but not limited to an individual's name, Social Security number, symbol, or other identifier assigned to the individual. (See Section 2.1 of this Handbook for details about what constitutes PII.) This section of the Handbook describes HUD SORN requirements.

6.1 SORN Templates and Reference Guide

HUD SORN templates and the **HUD SORN Reference Guide** can be found on the HUD Privacy Website. The Reference Guide provides detailed instructions and language examples for completing SORNs. **Please refer to the HUD SORN Reference Guide for a detailed, step-by-step guide for properly completing SORNs.**

6.2 What is a SORN?

A SORN is comprised of the Federal Register notice(s) that identifies the System of Records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system. The requirement for agencies and departments to publish a SORN allows the Federal Government to accomplish one of the basic objectives of the Privacy Act, fostering accountability through public notice.

6.3 Contents of a SORN:

A SORN must include:

- **a.** The name, location, and security classification of the system;
- **b.** The authority for the system;
- **c.** The purpose of the system;
- **d.** Whether any exemptions were promulgated for the system;
- **e.** The categories of individuals on whom records are maintained in the system;
- **f.** The categories of records maintained in the system;
- **g.** Each routine use of the records contained in the system, including the categories of users and the purpose of such use;
- **h.** The policies and practices of the department regarding storage, retrievability, access controls (such as administrative, technical, and physical safeguards), retention, and disposal of the records;
- **i.** The title and business address of the department official who is responsible for the System of Records;

j. The department procedures whereby an individual can be notified at his request if the System of Records contains a record pertaining to him;
k. The department procedures whereby an individual can be notified at his/her request how s/he can gain access to any record pertaining to their contained in the System of Records, and how s/he can contest its content; and
l. The categories of sources of records in the system.

6.4 Is a SORN Required?

- Do you collect or maintain information about individuals in a system that is retrieved by an individual identifier?
    - **If yes** → A SORN is required.
    - **If no** → A SORN is not required.

6.5 What Type of SORN Is Required?

- Is this a new System of Records or a modification to an existing system?
    - **New System of Records** → See **"New SORN"**
    - **Modification → See "Modified SORN"**
- Is a System of Records being terminated?
    - **If yes** → See **"Notice of Rescindment"**

6.5.1 Types of SORNs

New SORN – A new SORN is required when HUD establishes a new System of Records for which no prior Federal Register publication exists. The notice must be filed at least 30 days before the routine uses or disclosures are made from the System of Records.
Modified SORN – A modified SORN is required when a System of Records is significantly altered. Any new or significantly modified routine uses require a minimum of 30 days after publication in the Federal Register before the routine uses are effective and may be used as the basis for disclosure of a record in the system
Notice of Rescindment – A Notice of Rescindment must be filed when HUD stops maintaining a previously established System of Records. HUD shall publish a notice of rescindment in the Federal Register. A Notice of Rescindment must:

- Identify the System of Records
- Explain why the SORN is being rescinded and provide an account of what will happen to the records that were previously maintained in the system.
    - If the records in the System of Records will be combined with another System of Records or maintained as part of a new System of Records, the notice of rescindment shall direct members of the public to the SORN for the system that will include the relevant records.

6.5.2 SORNs – What Is a Significant Change?

Significant changes are those that are substantive in nature and therefore warrant a **Modified SORN** in order to provide notice to the public of the character of the modified System of Records. System Owners should contact their PLOs or Privacy Office before making a change to a System of Records to verify that the change is non-substantive. If the intended change is substantive, System Owners should work with PLOs and the Privacy Office to ensure that the SORN is modified to reflect that substantive change.

The following is a non-exhaustive list of examples of significant changes:

1. A substantial increase in the number, type, or category of individuals about whom records are maintained in the system. For example, a system covering physicians that is being expanded to include other types of health care providers (e.g., nurses or technicians) would require a revised SORN. Increases attributable to normal growth in a single category of individuals generally would not require a revised SORN.
2. A change that expands the types or categories of records maintained in the system. For example, a benefit system that originally included only earned income information that is being expanded to include unearned income information would require a revised SORN.
3. A change that modifies the scope of the system. For example, the combining of two or more existing systems of records.
4. A change that modifies the purpose(s) for which the information in the System of Records is maintained.
5. A change in the department's authority to maintain the System of Records or maintain, collect, use, or disseminate the records in the system.
6. A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute (e.g., to seek access to or amendment of a record).
7. A change to equipment configuration (either hardware or software), storage protocol, type of media, or department procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system. For example, a change in the access controls that substantially increases the accessibility of the information within the department.
8. A new routine use or significant change to an existing routine use that has the effect of expanding the availability of the information in the system.
9. The promulgation of a rule to exempt a System of Records from certain provisions of the Privacy Act.

6.5.3 Reports and Additional Documents that Accompany SORNs

New and Modified SORNs require additional reports and notices to be filed before the new system or modified system go into effect.

- **Report to Congress and OMB** – Upon establishment of a ***new*** *or* ***modified SORN***, copies of the SORN must be submitted to the Committee of Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, and OMB. The department provides advance notice to OMB and the committees of jurisdiction in Congress in order to permit an evaluation of the probable or potential effect of such a proposal on the privacy or other rights of individuals.
    - Pursuant to OMB Circular A-108, the reports to Congress and OMB must be completed ***at least 30 days before submission of notices to the Federal Register*** for publication.

- **Letter of Transmittal** – The transmittal letter serves as a ***brief cover letter*** accompanying the reports to Congress and OMB. The transmittal letter shall:
    a. Be signed by the SAOP.
    b. Contain the name, email address, and telephone number of the individual who can best answer questions about the proposed System of Records.
    c. Contain the Department's assurance that the proposed System of Records fully complies with the Privacy Act and OMB policies.
    d. Contain the Department's assurance that the proposed System of Records does not duplicate any existing department or government-wide systems of records.
- **Narrative Statement** – The narrative statement provides a ***brief overview of the proposed System of Records*** making reference to the other materials in the report without simply restating information provided in those materials. The narrative statement shall:
    a. Describe the purpose(s) for which the department is establishing or modifying the System of Records and explain how the scope of the system is commensurate with the purpose(s) of the system.
    b. Identify the specific authority (statute or executive order) under which the System of Records will be maintained. The Department shall avoid citing authority that is overly general; rather, the Department shall cite the specific programmatic authority for collecting, maintaining, using, and disseminating the information.
    c. An evaluation of the probable or potential effect of the proposal on the privacy of individuals whose information will be maintained in the System of Records. If the Department has conducted one or more privacy impact assessment(s) with respect to information technology that will be used to collect, maintain, or disseminate the information in the System of Records, the privacy impact assessment(s) will likely provide the information necessary to meet this requirement, and may be submitted in lieu of drafting a separate evaluation.

d. Explain how each new or modified routine use satisfies the compatibility requirement of the Privacy Act.
e. Identify any information collections approved by OMB or submitted to OMB for approval that will be used to collect information that will be maintained in the System of Records, and provide the relevant names, OMB control numbers, and expiration dates. If the request for OMB approval of an information collection is pending, the department may simply state the name of the collection and the date it was submitted to OMB for review.

- **Federal Register Notice** – The Privacy Act requires the Department to publish any new or modified routine use at least 30 days before the effective date of the routine use. The Department shall not disclose any records pursuant to a new or modified routine use until after the 30-day comment period has ended and the department has considered any comments from the public and determined that no further modifications are necessary.
- **Exemption Rule** – Any new Privacy Act exemption rules or changes to published exemption rules in Federal Register that the department proposes to issue that will apply to records in the new or significantly modified System of Records. See Section 4.7 of this Handbook for details regarding Privacy Act Exemptions.
- **Supplementary Documents** – The supplementary documents include:
  - For significantly modified systems, the Department shall include a list of the substantive changes to the previously published version of the notice and/or a version of the previously published notice that has been marked up to show the changes that are being proposed.
  - The Department shall include any other supplementary documents requested by OMB.

6.5.4 Establishing or Modifying a SORN

It is HUD's policy to publish a SORN in the Federal Register for any department-maintained information technology (IT) or paper file system that contains information about individuals and retrieves information by a personal identifier. Use the HUD SORN Templates to provide the Privacy Office with necessary information.

6.5.5 Rescinding a SORN

A System of Records is terminated whenever the information is no longer accessed by individuals' names or other identifiers, or whenever it is consolidated with another System of Records. Terminating a system may involve the physical destruction of records; it may involve purging the system of individual identifiers and maintaining the data in another form, such as statistical data; and it may involve altering the manner in which the records are accessed so that records are no longer accessed by the name of the subject individuals or other personal identifiers.

When a System of Records is terminated, a **Notification of Rescindment** should be sent to the Privacy Office for record keeping and for publication in the Federal Register.

Any time a SORN is rescinded, the System Owner should check to ensure that the accompanying PIA is also retired. See Section 5.0 for details.

6.6 SORN Exemptions

In order for HUD to exercise the provisions of these exemptions, notice of proposed rulemaking must be published in the Federal Register.

Each exemption rule submitted for publication must contain:

a. The record system identifier and system name of the system for which the exemption is claimed;
b. The specific sections of the Privacy Act under which the exemption for the system is claimed;
c. The specific sections of the Privacy Act from which the system is to be exempted; and
d. The specific reasons why an exemption is being claimed from each section of the Act identified.

The Privacy Office must publish all exempted System of Records on HUD's SORN webpage. The publication must include:

a. The name of the system
b. Links to all SORNs relating to the exempted System of Records.

7.0 Computer Matching Agreements (CMA)

The Privacy Act requires agencies and departments engaged in computer matching activities to provide notice to individuals if their information is being computer matched. Individuals must be provided with the opportunity to refute adverse information before having a benefit denied or terminated on the basis of a match. Agencies departments are required to establish a Data Integrity Board (DIB) to oversee computer matching activities.

7.1 What Is a CMA?

A CMA is a written agreement establishing the conditions, safeguards, and procedures under which a Federal agency or department agrees to disclose data with another Federal or state agency when there is a computerized comparison of two or more automated System of Records for the purpose of determining eligibility for a benefit.

A **Federal Matching Notice** for each CMA must be published by the Department in the Federal Register upon the ***establishment, re-establishment, or modification of a matching program*** that describes the existence and character of the matching program. A matching notice identifies the agencies involved, the purpose(s) of the matching program, the authority for conducting the matching program, the records and individuals involved, and additional details about the matching program.

- Matching notices must be ***filed to the Federal Register 30 days before the notice goes into effect***. This 30-day period allows for public comment. HUD

must review all public comments on the notice and determine whether any changes to the matching notice are necessary.
    - If needed, HUD will publish a revised matching notice and allow for a further 30-day comment period.

7.2 Contents of a CMA

Per OMB Circular A-108, a CMA must Include:

a. The purpose and legal authority for conducting the program;
b. The justification for the program and the anticipated results, including a specific estimate of any savings;
c. A description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;
d. Procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the DIB of such agency or department (subject to guidance provided by the Director of OMB) to—
    1. Applicants for and recipients of financial assistance or payments under Federal benefit programs, and
    2. Applicants for and holders of positions as Federal personnel, that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;
e. Procedures for verifying information produced in such matching program;
f. Procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;
g. Procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
h. Prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;
i. Procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;
j. Information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
k. That the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

7.3 Is a CMA Required?

- Is the information to be shared contained in a System of Records?
  - **If yes** → Will the information be used to compare information held by another agency to make a determination concerning eligibility for benefits?
    - **If no** → Then a CMA is **not required**.
    - **If yes** → Then a CMA **is required.**
  - **If no** → A CMA is **not required**.

7.4 What Type of CMA Is Required?

- Is this a new matching program?
  - **If yes** → See "**New Agreement**"
  - **If no** → Is this matching agreement going to expire in 3 months or less?
    - **If yes** → Is this matching program less than 18 months old?
      - **If yes** → See "**Renewal Agreement**"
      - **If no** → See "**Re-Establishment Agreement**"
    - **If no** → Are significant changes being made to the existing matching agreement?
      - **If yes** → See "**Modified Agreement**"

7.4.1 Types of CMAs

- **New Agreement** – A new agreement is used the first time a matching agreement is developed for a matching program. The matching agreement may exist for up to 18 months and may be extended 12 additional months. A new agreement must be reviewed by the DIB and requires development of a cost-benefit analysis.
  - **Cost-benefit Analysis** – The process whereby the recipient agency measures the benefits of engaging in a proposed CMA and compares the benefits with the costs. Benefits may include the avoidance of future improper and the recovery of improper payments and debts. Costs may include personnel costs (e.g., salaries) and computer costs related to the processing of computer matching (e.g., maintenance and use of computers at facilities).
- **Modified Agreement** – A modified agreement is used when the department is making significant changes to an existing matching program. See Section 7.4 of this Handbook for details
- **Renewal Agreement** – An extension agreement allows the continuation of an existing initial agreement for an additional 12 months, without additional review by the DIB, provided certain conditions are met.
  - The participating agencies must certify to the Chairperson of the DIB that the matching program will be continued in full compliance with the existing agreement and requested within the last 90 days of the existing agreement.

- Notices and reports are not required.

- **Re-Establishment Agreement** – When the initial matching agreement (including any extension) has expired, a renewal agreement permits the matching program to continue and may exist for up to 18 months. This agreement must be approved by the DIB within the last 90 days of the existing agreement to prevent the match from lapsing. Requires the same review, reports and notices as a new agreement.

7.4.2 CMAs – What is a Significant Change?

Significant changes are those that are substantive in nature and therefore warrant a revision of the matching notice in order to provide notice to the public of the modified matching program. The following are non-exhaustive examples of significant changes:

a. A change that modifies the purpose(s) of the matching program.
b. A change in the department's authority to conduct the matching program.
c. A change that expands the types or categories of records that are used in the matching program, or a significant increase in the number of records that are being matched.
d. A change that expands the categories of individuals whose records are used in the matching program.
e. A change to the source and/or recipient agencies that are involved in the matching program.

7.4.3 Reports and Additional Documents for CMAs

New, Modified, and Re-Establishment CMAs require additional reports and notices to be filed before the matching program goes into effect.

- **Report to Congress** – Upon establishment of a ***new, re-establishment, or significantly modified matching agreement***, copies of the matching agreement must be submitted to the Committee on Homeland Security Governmental Affairs of the Senate and Committee on Oversight and Government Reform of the House of Representatives. Agencies provide advance notice to OMB and the committees of jurisdiction in Congress in order to permit an evaluation of the probable or potential effect of such a proposal on the privacy or other rights of individuals.
  - Pursuant to OMB Circular A-108, the reports to Congress must be completed ***at least 30 days before submission of matching notices to the Federal Register*** for publication.
- **Letter of Transmittal** – The transmittal letter serves as a ***brief cover letter*** accompanying the report to Congress. The transmittal letter shall:
  a. Be signed by the SAOP or the Chairperson of the DIB.
  b. Contain the name, email address, and telephone number of the individual who can best answer questions about the proposed matching program.
  c. Contain the department's assurance that the proposed matching program fully complies with the Privacy Act and OMB policies.

- **Narrative Statement** – The narrative statement provides a ***brief overview of the proposed matching program*** making reference to the other materials in the report without simply restating information provided in those materials. The narrative statement shall:
    a. Describe the purpose(s) for which the department is establishing, re-establishing, or significantly modifying the matching program.
    b. Identify the specific authority (statute or executive order) under which the department is conducting the matching program. The department shall avoid citing authority that is overly general; rather, the department shall cite the specific programmatic authority for conducting the matching program.
    c. Describe the administrative, technical, and physical safeguards in place to protect against unauthorized access to records used in the matching program.
    d. Provide the department's specific evaluation of the potential impact on the privacy of individuals whose records will be used in the matching program.
    e. Indicate whether a cost-benefit analysis was performed for the matching program, describe the results of the cost-benefit analysis, and explain the basis on which the department is justifying the matching program.
- **Supplementary Documents** – The supplementary documents include:
    - For significantly modified matching programs, the department shall include a list of the substantive changes to the previously published version of the matching notice and/or a version of the previously published matching notice that has been marked up to show the changes that are being proposed.
    - The department shall include any other supplementary documents requested by OMB.

7.5 CMA Procedures and Timing

This section of the Handbook provides guidelines for when to begin drafting CMAs and CMA-related documentation for each type of CMA.

7.6 Procedures for New and Significantly Modified CMAs

Action	Timing
HUD Program Office works with the HUD Privacy Office to: • Draft a new CMA or update the existing CMA. • Draft the transmittal letters to both Houses of Congress and OMB. • Draft the Federal Register notice. • Draft a narrative statement for the new or updated CMA. • Draft the cost-benefit analysis (CBA) (if necessary). • If this is a Significantly Modified CMA, include a list of the substantive changes to the previously published version of the matching notice and/or a version of the previously published matching notice that has been marked up to show the changes that are being proposed.	Begin drafting approximately 280 days before the intended implementation date of the matching program.
HUD Program Office submits the agreement to the **HUD Privacy Office**.	At least 100 days before the intended implementation date of the matching program.
The **HUD Data Integrity Board (DIB)** approves the matching agreement and the **HUD DIB Chairperson** signs the matching agreement.	At least 90 days before the intended implementation date of the matching program.
The **Other Matching Agency's DIB** approves and signs the matching agreement and returns it to the **HUD Privacy Office** and **CPO**.	Allow 3-4 weeks for approval and signing.

Action	Timing
The **HUD CPO** immediately submits 2 copies of the matching agreement along with the respective transmittal letters to **both Houses of Congress** and the **OMB**. **Submit to:** • **The Administrator of the Office of Information and Regulatory Affairs** within the OMB via the ROCIS system. • **House Committee on Oversight and Government Reform** o 2157 Rayburn House Office Building, Washington, DC 20515 • **Senate Committee on Homeland Security and Governmental Affairs** o 340 Dirksen Senate Office Building, Washington, DC 20510	At least 60 days before the intended implementation date of the matching program.
The **OMB** and **Congress** evaluates the matching agreement.	The standard review period is 30 days.
Once the **OMB** and **Congress** approve of the matching agreement, the **HUD CPO**, or the partner agency when HUD is the source agency for the match, files a matching notice with the Federal Register for publication.	At least 30 days before the intended implementation date of the matching program.

Table 2. Procedures for New and Significantly Modified CMAs

7.7 Procedures for Re-Establishment CMAs

Action	Timing
HUD Program Office works with the **HUD Privacy Office to:** • Draft the CMA or update the existing CMA. • Draft the transmittal letters to both Houses of Congress and OMB. • Draft the Federal Register notice when necessary. • Draft a narrative statement for the new or updated CMA. • Draft the cost-benefit analysis (CBA) (if necessary).	Begin drafting 190 to 220 days before the expiration date of the matching agreement.
HUD Program Office submits the agreement to the **HUD Privacy Office**.	At least 100 days before the intended implementation date of the matching program.
The **HUD DIB** approves the matching agreement and the **HUD DIB Chairperson** signs the matching agreement.	At least 90 days before the intended implementation date of the matching program.
The **Other Matching Agency's DIB** approves and signs the matching agreement and returns it to the **HUD Privacy Office** and **CPO**.	Allow 3-4 weeks for approval and signing.

Action	Timing
The **HUD CPO** immediately submits 2 copies of the matching agreement along with the respective transmittal letters to **both Houses of Congress** and the **OMB**. **Submit to:** • **The Administrator of the Office of Information and Regulatory Affairs** within the OMB via the ROCIS system. • **House Committee on Oversight and Government Reform** o 2157 Rayburn House Office Building, Washington, DC 20515 • **Senate Committee on Homeland Security and Governmental Affairs** o 340 Dirksen Senate Office Building, Washington, DC 20510	At least 60 days before the intended implementation date of the matching program.
The **OMB** and **Congress** evaluates the matching agreement.	The standard review period is 30 days.
Once the **OMB** and **Congress** approve of the matching agreement, the **HUD CPO** or the partner agency if HUD is the source agency for the match files a matching notice with the Federal Register for publication.	At least 30 days before the intended implementation date of the matching program.

Table 3. Procedures for Re-Establishment CMAs

7.8 Procedures for Renewal CMAs

Action	Timing
If **HUD Program Office** and **Other Matching Agency** drafts an agreement in writing, certifying to the **HUD DIB** that: • The matching program will be conducted without any change • The program has been conducted in compliance with the agreement.	120-130 days before the expiration of the CMA.

Action	Timing
HUD Program Office submits the agreement to the **HUD Privacy Office**.	Within 90 days of the expiration of the matching agreement.
The **HUD DIB** approves the extension agreement, allowing the matching program to continue an addition 12 months from the date the original CMA expires. No notices or reports are necessary.	Within 90 days of the expiration of the matching agreement.

Table 4. Procedures for Renewal CMAs

7.9 CMA Review and Maintenance

Existing CMAs should be continuously monitored to ensure extensions, renewals, and modifications are submitted in a timely manner. System Owners should also notify PLOs of violations of CMA terms for systems they own. PLOs should report violations to the Privacy Office.

7.10 CMA Website Publication

The Privacy Office shall provide links on the HUD Privacy Website to matching notices and agreements for all active matching programs in which HUD participates.

7.11 Data Integrity Board

The Privacy Office establishes and maintains a DIB to oversee and manage CMAs. The DIB reviews and approves CMAs involving the various HUD Offices on behalf of the Department, including drafting, approval, and revision of CMAs. This section of the Handbook describes the responsibilities and membership requirements of the DIB.

7.11.1 DIB Responsibilities

The HUD DIB:

1. Oversees and coordinates the review, approval, maintenance, reporting and compliance of all HUD CMAs with applicable laws, regulations, guidelines, and existing CMAs;
2. Reviews, approves (by majority vote), and maintains all written agreements for receipt or disclosure of department records for matching programs to ensure compliance with all relevant statutes, regulations, and guidelines;
3. Reviews all matching programs in which the department has participated during the year, either as a source agency or recipient agency, to determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assesses the costs and benefits of such programs;
4. Reviews all recurring matching programs in which the department has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

5. Submits an annual report, compiled by the CPO, which is then submitted to the Secretary of Homeland Security and the Director of OMB, and published on the HUD website, describing the matching activities of the department, including:
    a. Matching programs in which the department has participated as a source agency or recipient agency;
    b. Matching agreements proposed that were disapproved by the DIB;
    c. Any changes in membership or structure of the DIB in the preceding year;
    d. The reasons for any waiver of requirements for completion and submission of a cost-benefit analysis prior to the approval of a matching program;
    e. Any violations of matching agreements that have been alleged or identified and any corrective action taken; and
    f. Any other information required by the Director of OMB to be included in such report.
6. Serves as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;
7. Provides interpretation and guidance, through the CPO, to HUD Components and personnel on the requirements for matching programs; and
8. Reviews HUD recordkeeping and disposal policies and practices for matching programs to assure compliance with Federal requirements.
9. May review and report on any agency matching activities that are not matching programs.

7.11.2 DIB Membership

The SAOP will designate members to the DIB as needed, as long as the following mandatory positions are filled:

1. **Chairperson**
    - This position must be filled by either the SAOP or CPO.
2. **Inspector General**
    - The Inspector General must be on the DIB but may not serve as Chairperson.
3. **Secretary**
    - One member of the DIB must be designated as the Secretary of the DIB for purposes of the Annual CMA Activity Report but may also hold other positions on the DIB.
4. **Counsel to the DIB**
    - A member from the Office of General Counsel (OGC) must serve as the counsel to the DIB to ensure proper legal support for CMA reviews.

8.0 Federal Reporting Requirements

8.1 Annual Computer Matching Agreement (CMA) Activity Report

Per OMB Federal reporting requirements, HUD must submit an Annual CMA Activity Report that accounts for all matching programs HUD engaged in during the reporting year.

The Privacy Office is responsible for consolidating information and submitting the activity report. All HUD offices are responsible for coordinating with their PLOs to compile necessary information for the annual activity report.

All HUD offices are responsible for ensuring that CMAs sent to the Privacy Office in a timely manner. See Section 7.5 of this Handbook for details regarding CMA schedules and notice types. PLOs are responsible for tracking any violations of any CMA terms and reporting them to the Privacy Office for inclusion in the Annual CMA Activity Report.

Please refer to the Computer Matching Agreement (CMA) Activity Report Guide and template regarding the types of information that may need to be provided to the Privacy Office.

8.2 Annual SAOP FISMA Report

Federal agencies are required to submit the annual Senior Agency Official for Privacy (SAOP) report to OMB pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). Each year, OMB issues guidance instructing each SAOP to review the administration of the department's Privacy Program and report compliance data to OMB. Per OMB requirements, HUD SAOP is required to report on specific metrics and submit privacy program documentation through CyberScope. Please refer to the Annual SAOP FISMA Report Reference Guide for details on the process. The guide and associated templates are available on the HUD Privacy SharePoint.

8.3 Annual SAOP FISMA Metrics

At the beginning of the reporting year (no later than November 30), the Privacy Office will confirm the relevant metrics, documents, and deadlines for submitting the SAOP report via CyberScope and OMB guidance. HUD Offices, PLOs, and System Owners are responsible for coordinating to provide the Privacy Office with any information needed to fill and submit the report. The following table includes the metrics and information that HUD Offices will need to provide to the Privacy Office.

Document Name	Description	Due By	Point of Contact
HUD's Privacy Program Plan	HUD's Privacy Program Plan, which can be found on the HUD Privacy Website.	No later than (NLT) one week before draft SAOP report is routed for department approvals	Privacy Office
Privacy Program Changes	Major changes made to HUD's privacy program during the reporting period, including changes in leadership, staffing, structure, and organization	NLT one week before draft SAOP report is routed for department approvals	Privacy Office
HUD's Agency Breach Response Plan	Major changes made to HUD's privacy program during the reporting period, including changes in leadership, staffing, structure, and organization	Due to Privacy Office NLT one month before the SAOP report is routed for department approvals	Privacy Office, OCIO
HUD's privacy continuous monitoring strategy	HUD's current continuous monitoring strategy	Due to Privacy Office NLT one month before the SAOP report is routed for department approvals	Privacy Office, OCIO
Privacy program webpage(s)	The Uniform Resource Locator (URL) for HUD's public-facing Privacy Program page, as well as the URL for any other sub-agency-, component-, and/or program-specific privacy program pages, as well as links to the public-facing privacy policy repository	NLT one week before the SAOP report is routed for department approvals	Privacy Office

Social Security Number (SSN) collection policy	The agency's written policy to ensure that any new collection or use of Social Security numbers (SSNs) is necessary	Due to Privacy Office NLT one month before the SAOP report is routed for department approvals	Privacy Office, OCIO

Table 5. Annual SAOP FISMA Report Metrics

8.4 Annual SAOP FISMA Timeline

In order to ensure timely consolidation of information from across HUD Offices, the following table provides the timeline for when information will need to be gathered and submitted to the Privacy Office.

Action	Due By	Point of Contact
Confirm the relevant metrics, documents, and deadlines for submitting the SAOP report via CyberScope and OMB guidance	November 30 of reporting year	Privacy Office
Inform SAOP of reporting requirements / deadlines for reporting year	January 15th of reporting year	Privacy Office
Draft internal schedule for collecting all required metrics and documentation and share with SAOP for approval	January 15th of reporting year	Privacy Office
Share the required reporting metrics, documentation, and due dates with the Privacy Liaison Officers (PLOs)	January and February PLO Meetings	Privacy Office
Collect documents and metrics available and coordinate with the appropriate Program Offices, through their respective PLOs, to identify remaining artifacts / information needed for the full report.	Two months before CyberScope submission deadline	Privacy Office, PLOs

Program Offices must submit any and all remaining artifacts/information needed for the full report as soon as possible after items have been identified.		
Complete a draft of SAOP report and submit draft for agency review and comment	One month before CyberScope submission deadline	Privacy Office
SAOP conducts final review, approval, and submission of the full Report	One week before CyberScope submission Deadline	Privacy Office

Table 6. Annual SAOP FISMA Report Timeline

9.0 Forms and Contracts Requirements

9.1 Privacy Act Statements

The Privacy Act requires that HUD provide to any individual from whom it collects information as part of a system of records with the following:

a. The authority (whether granted by statute or by Executive Order of the President) for soliciting the information and whether disclosure is mandatory or voluntary;
b. The principal purpose(s) for which the information is intended to be used;
c. The routine use(s) for which the information may be used, as published in the System of Records Notice (SORN),
d. The effects on the individual, if any, of not providing all or any part of the requested information; and
e. An appropriate citation (and, if practicable, a link) to the relevant SORN(s) (Pursuant to OMB Circular A-108).

The information above must be included on the information collection form itself, or in a separate form which can be retained by the individual whose information is being collected.

The following is an explanation for what each element of the Privacy Act Statement should include:

- **Authority – Legal authorities that permit collection. This information is available in the SORN for each system of records.**
- **Disclosure** – Acknowledge whether the information is mandatory or voluntary, and the consequences of not providing the requested information.

  - Disclosure is typically voluntary within HUD. A collection is only mandatory if required by law. For example, the consequence of not providing information can result in the individual being unable to complete an application. However, the collection itself is still voluntary because the individual can choose to not complete the application. In this example, the effect of not providing the information may be a delay in processing or denial of the application.

- **Principal Purpose** – Main purpose of system or data collection and why it is being collected.
- **Routine Use(s)** – Where the information will be disclosed outside of HUD, and to whom it will be disclosed.
- **System of Records Notice** – URL and citation where the SORN for the form or system can be accessed. The following citation information can be found on the right-hand side of each Federal Register SORN webpage.
  - **Document Citation**
  - **Document Number**
  - **Docket Number**

9.2 Privacy Advisory Statements

Privacy Advisory Statements are required when soliciting an individual's SSN for authentication purpose only and **will not be maintained in a System of Records**. The Privacy Advisory Statement informs the individual why the information is being solicited and how it will be used.

a. The authority (whether granted by statute or by Executive Order) for soliciting the information and whether disclosure is mandatory or voluntary;
b. The principal purpose(s) for which the information is intended to be used; and
c. The effects on the individual, if any, of not providing all or any part of the requested information.

The information above must be included on the information collection form itself, or in a separate form which can be retained by the individual whose information is being collected.

9.3 Contracts

HUD procures a variety of services from the private sector and provides grants to individuals and outside organizations. As many of these procurements may trigger the applicability of Privacy Act requirements, the following standard language must be customized and included in all HUD contracts:

1. The Contractor shall maintain compliance with all current and future Federal IT security requirements. The Contractor shall:

A. Use, maintain, enhance, develop and upgrade all information technology software and system documentation under this Contract in accordance with Federal Laws, best practices, and regulations. This includes, but is not limited to:
    i. Federal Information Security Modernization Act - https://www.congress.gov/bill/113th-congress/senate-bill/2521;
    ii. The Privacy Act - https://www.archives.gov/about/laws/privacy-act-1974.html;
    iii. The E-Government Act - https://www.archives.gov/about/laws/egov-act-section-207.html;
    iv. The Clinger-Cohen Act - https://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf;
    v. Paperwork Reduction Act - https://www.law.cornell.edu/uscode/text/44/3501;
    vi. Office of Management and Budget Circulars A-130, and A-I23 - https://www.whitehouse.gov/omb/information-for-agencies/circulars/;
    vii. Office of Management and Budget Memorandum 17-12 - https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf;
    viii. Department of Housing and Urban Development regulations, Handbooks and Policies - https://www.hud.gov/program_offices/officeofadministration/privacy_act/pia/polyref;
    ix. GAO directives - https://www.gao.gov/index.html; and
    x. Federal Financial Manager Integrity Act (FFMIA) - https://obamawhitehouse.archives.gov/omb/financial_ffs_ffmia.

B. Maintain Security Assessment and Authorization (SA&A) standards in accordance with guidance published by NIST. An independent SA&A will be performed by Housing and Urban Development (HUD) during the period of performance of this contract. The Contractor shall complete the SA&A within [*time period consistent with contract terms, e.g. three weeks, six months, etc.*] after the award of the contract and again at the expiration of the SA&A and to include any revisions or updates.

C. Follow HUD's Project Planning and Management (PPM) Life Cycle and industry best practices in the analysis, design, development, testing and implementation of proposed new systems and/or the enhancement to existing systems. This includes prohibiting live data from being used in any environment other than Production and Disaster Recovery (DR) environments. Specifically, no live data should be used in development, testing or staging environments.

D. Review and update system documentation to ensure accuracy, compliance and completeness. Reviews and revisions must be completed and delivered to HUD quarterly.

E. The Contractor will prepare its security plan as part of its demonstration that it meets the requirements for SA&A per the applicable requirements from HUD, OMB, NIST, etc., which will require the preparation of several related documents, including but not limited to:
    i. NIST FIPS 199/200 Security Categorization Analysis;
    ii. NIST SP-800 Security Controls Self-Assessment;
    iii. Application and network vulnerability scans;
    iv. Business Impact Assessment;
    v. Privacy Impact Assessment;
    vi. Create System Security Plan, Risk Assessment, Technical Architecture, COOP and Contingency Plans, Quality Control Plan, ST&E Plan and other relevant SA&A supporting documentation for each new application;
    vii. Security Assessment Tests (formerly ST&E Testing);
    viii. Security Assessment Reports (formerly ST&E Report);
    ix. POA&M; and
    x. Accreditation Documentation.

F. Each mixed or financial system that the contractor manages, develops, modifies, enhances, releases and/or upgrades will be assessed under the Federal Information System Controls Audit Manual (FISCAM) methodology that include control families for both General Computer and Business Process Application controls:
    i. General Controls:
        1. Security Management
        2. Access Controls
        3. Configuration Management
        4. Segregation of Duties
        5. Contingency Planning
    ii. Business Process Application Controls:
        1. Application Security
        2. Business Process Controls
        3. Interfaces
        4. Data Management

G. Each mixed or financial system that the contractor manages, develops, modifies, enhances, releases and/or upgrades must comply with identified OMB A-123 Appendix A "Management's Responsibility for Internal Control", and Appendix D “Compliance with the Federal Financial Management Improvement Act of l996” key controls; and the Federal Information Security Management Act of 2002 (FISMA) to include:
    i. National Institute of Standards and Technology Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5 (NIST SP 800-53, Rev. 5);
    ii. NIST SP 800-18 Rev. 1 - Guide for Developing Security Plans for Federal Information Systems;
    iii. NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments;

iv. NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems;
v. NIST SP 800-37 Rev. 2 - Guide for Applying the Risk Management Framework to Federal Information Systems;
vi. NIST SP 800-47 Rev. 1 - Security Guide for Interconnecting Information Technology Systems
vii. NIST SP 800-53A Rev. 5 - Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans;
viii. NIST SP 800-59 - Guideline for Identifying an Information System as a National Security System;
ix. NIST SP 800-60 Rev. 1 - Guide for Mapping Types of Information and Information Systems to Security Categories;
x. NIST SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
xi. Federal Information Processing Standards (FIPS) 199/200 - Security Categorization Analysis; and
xii. FIPS 191 - Guideline for the Analysis of Local Area Network Security.

2. HUD's Office of the Chief Information Officer (OCIO) will have responsibility for maintaining the FISCAM-based mapping of security controls that will be required in order to maintain compliance with FISMA, OMB A-123, and HUD security requirements.

3. The Contractor shall support and provide system security to ensure availability, confidentiality, and integrity of the HUD data applications (e.g. maintaining access control, user identification, password protection and authentication, confidentiality of customer profiles and traffic, physical and personnel security required under this PWS). Provide SA&A support, including potential off cycle or unanticipated SA&A support, over the life of the contract.

4. The HUD System Security Plans (Risk Assessment, Incidence Response Plan and IT Contingency Plan) shall be reviewed and presented to HUD's Chief Information Security Officer for approval.

5. The Contractor shall maintain compliance with OMB Memorandum 17-12 (OMB M 17-12), which requires contractors and sub-contractors (at any tier) to:
   A. Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
   B. Properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies and to comply with any agency-specific policies for protecting PII;

C. Provide and participate in mandatory training on how to identify and report a breach;
D. Report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;
E. Maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;
F. Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with OMB M 17-12, the agency's breach response plan, and to assist with responding to a breach;
G. Identify roles and responsibilities, in accordance with OMB M 17-12 and the agency's breach response plan; and,
H. Explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

6. The Contractor shall provide and present a Security Self-Assessment Report to HUD's Chief Information Security Officer on an annual basis, due no later than August 31st of each calendar year.

7. Plans of Action and Milestones (POA&Ms) shall be reviewed and updated on a [*timeframe that is consistent with contract terms, e.g. quarterly, annual, bi-monthly, etc.*] basis and presented to HUD's Chief Information Security Officer for review and approval.

8. Failure to adhere to the above NIST requirements could result in penalties, to include a contract performance stop-work order until compliance can be demonstrated. Disregard of these NIST requirements could also lead to other criminal, civil, administrative, or contract penalties, including, but not limited to:
   A. Breach of Contract damages
   B. False Claims Act damages
   C. Liquidated Damages
   D. Termination for Default
   E. Termination for Convenience
   F. Poor Past Performance
   G. Suspension/debarment

Appendix A. Authorities and References

1. Privacy Act of 1974, 5 U.S.C. § 552a, December 31, 1974

2. E-Government Act of 2002, Public Law 107-347, Section 208, December 17, 2002

3. Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. § 3551, et seq., December 18, 2014

4. OMB, Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, December 23, 2016

5. OMB, Circular A-130, Managing Information as a Strategic Resource, July 28, 2016

6. OMB, Memorandum 21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act, November 12, 2020

7. NIST, SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020 (includes updates as of Dec. 10, 2020)

8. NIST, SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010

Appendix B. Acronyms

Acronym	Definitions
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMA	Change Management AgreementC
CMPPA	Computer Matching and Privacy Protection Act
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DIB	Data Integrity Board
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
HUD	US Department of Housing and Urban Development
NARA	National Archives and Records Administration
NIST	National Institute of Standards & Technology
OGC	Office of General Counsel
OIG	Office of the Inspector General
OITS	Office of Information Technology Services
OMB	Office of Management and Budget
PLO	Privacy Liaison Officer
POA&Ms	Plan of Action & Milestones
SA&A	Security Assessment and Authorization
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
SSN	Social Security Number
RMLO	Records Management Liaison Officers