

Senior Agency Official For Privacy

2022
Annual Report

Department of Housing and Urban Development

Section 1: General Privacy Program Requirements

- 1a. Has the head of the agency designated a Senior Agency Official for Privacy (SAOP), as required by Executive Order 13719 and OMB guidance?
- Yes
- 1b. Has the agency reported the name, title, and contact information of the current SAOP to OMB on the MAX website of the Federal Privacy Council? (Indicate "N/A" if the agency has not designated an SAOP.)
- Yes
- 1c. Does the SAOP have the necessary position, expertise, and authority to serve in the role of SAOP? (Select all that apply or indicate "N/A" if the agency has not designated an SAOP.)
- Position
 - Expertise
 - Authority
- 1d. Does the SAOP have the necessary role and responsibilities within the agency for each of the following? (Select all that apply or indicate "N/A" if the agency has not designated an SAOP.)
- Policy making
 - Compliance
 - Risk management activities
- 1e. Has the agency developed and maintained a privacy program plan?
- Yes
- 1f. Does the agency's privacy program plan include a description of each of the following? (Select all that apply or indicate "N/A" if the agency has not developed and maintained a privacy program plan.)
- Structure of the privacy program
 - Resources dedicated to the privacy program
 - Role of the SAOP and other privacy officials and staff
 - Strategic goals and objectives of the privacy program
 - Program management and common controls in place or planned for meeting applicable privacy requirements and management privacy risks

Section 2A: Information Systems

Section 2A: Information Systems

- 2a. Does the agency maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII)?

Yes

Section 2B: Information Systems

- 2b. Number of information systems reported in response to question 1.1 of the FY 2022 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

		2b. Number of information systems reported in response to question 1.1 of the FY 2019 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).			2c. Number of information systems reported in question 2b that the agency authorized or reauthorized to operate during the reporting period.			2d. Number of information systems reported in question 2c where the SAOP reviewed and approved the categorization of the information system in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60.			2e. Number of information systems reported in question 2c where the SAOP reviewed and approved a system privacy plan for the information system prior to the information system's authorization or reauthorization.			2f. Number of information systems reported in question 2c where the SAOP conducted and documented the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented for the information system prior to the information system's authorization or reauthorization.			2g. Number of information systems reported in question 2c where the SAOP reviewed the information system's authorization package to ensure compliance with applicable privacy requirements and manage privacy risks, prior to the authorizing official making a risk determination and acceptance decision.		
Bureau/ Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
ADMIN	In Progress	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
CFO	In Progress	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2
CPD	In Progress	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2
CPO	In Progress	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2
ODOC	In Progress	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ENFC	In Progress	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FHEO	In Progress	3	0	3	3	0	3	3	0	3	3	0	3	3	0	3	3	0	3
GNMA	In Progress	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HSG	In Progress	17	0	17	17	0	17	17	0	17	17	0	17	17	0	17	17	0	17

Section 2B: Information Systems

		2b. Number of information systems reported in response to question 1.1 of the FY 2019 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).			2c. Number of information systems reported in question 2b that the agency authorized or reauthorized to operate during the reporting period.			2d. Number of information systems reported in question 2c where the SAOP reviewed and approved the categorization of the information system in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60.			2e. Number of information systems reported in question 2c where the SAOP reviewed and approved a system privacy plan for the information system prior to the information system's authorization or reauthorization.			2f. Number of information systems reported in question 2c where the SAOP conducted and documented the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented for the information system prior to the information system's authorization or reauthorization.			2g. Number of information systems reported in question 2c where the SAOP reviewed the information system's authorization package to ensure compliance with applicable privacy requirements and manage privacy risks, prior to the authorizing official making a risk determination and acceptance decision.		
Bureau/ Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
OCIO	In Progress	8	0	8	8	0	8	8	0	8	8	0	8	8	0	8	8	0	8
OGC	In Progress	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OIG	In Progress	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
PDR	In Progress	5	0	5	5	0	5	5	0	5	5	0	5	5	0	5	5	0	5
PIH	In Progress	11	0	11	11	0	11	11	0	11	11	0	11	11	0	11	11	0	11
REAC	In Progress	7	0	7	7	0	7	7	0	7	7	0	7	7	0	7	7	0	7
ODEEO	In Progress	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
FPM	In Progress	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
OPA	In Progress	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<i>Agency Totals</i>		61	0	61	61	0	61	61	0	61	61	0	61	61	0	61	61	0	61

Section 3A: Information Technology Systems and Privacy Impact Assessments

3a. Does the agency maintain an inventory of the agency's information technology (IT) systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

Yes

Section 3B: Information Technology Systems and Privacy Impact Assessments

Section 3B: Information Technology Systems and Privacy Impact Assessments

- 3b. Number of IT systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a privacy impact assessment (PIA) under the E-Government Act of 2002.

		3b. Number of IT systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a privacy impact assessment (PIA) under the E-Government Act of 2002.			3c. Number of IT systems reported in question 3b that are covered by an up-to-date PIA.		
Bureau/ Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
ADMIN	In Progress	1	0	1	1	0	1
CFO	In Progress	2	0	2	2	0	2
CPD	In Progress	2	0	2	2	0	2
CPO	In Progress	2	0	2	2	0	2
ODOC	In Progress	0	0	0	0	0	0
ENFC	In Progress	0	0	0	0	0	0
FHEO	In Progress	3	0	3	3	0	3
GNMA	In Progress	0	0	0	0	0	0
HSG	In Progress	17	0	17	17	0	17
OCIO	In Progress	8	0	8	8	0	8
OGC	In Progress	0	0	0	0	0	0
OIG	In Progress	1	0	1	1	0	1
PDR	In Progress	5	0	5	5	0	5
PIH	In Progress	11	0	11	11	0	11
REAC	In Progress	7	0	7	7	0	7
ODEEO	In Progress	1	0	1	1	0	1
FPM	In Progress	0	0	0	0	0	0
OPA	In Progress	0	0	0	0	0	0
Agency Totals		60	0	60	60	0	60

Section 3C: Information Technology Systems and Privacy Impact Assessments

- 3d. Does the agency have a written policy for PIAs that includes each of the following? (Select all that apply or indicate "N/A" if the agency does not have a written policy for PIAs.)
- A requirement that a PIA be conducted and approved prior to the development, procurement, or use of an IT system that requires a PIA
 - A requirement that system owners, privacy officials, and IT experts participate in conducting PIAs
 - A requirement for PIAs to be updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks associated with the use of a particular IT system
- 3e. Does the agency have a process or procedure for each of the following? (Select all that apply.)
- Assessing the quality and thoroughness of each PIA
 - Performing reviews to ensure that appropriate standards for PIAs are maintained
 - Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated
 - Ensuring that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks

Section 4: Systems of Records

- 4a. Number of Privacy Act systems of records maintained by the agency during the reporting period (including those operated by a service provider or a contractor on behalf of the agency).
- 29
- 4b. Number of Privacy Act systems of records reported in question 4a for which an up-to- date system of records notice (SORN) has been published in the Federal Register.
- 29
- 4c. Does the agency have a process for determining whether a new or revised SORN is required when the agency collects or maintains information about individuals?
- Yes
- 4d. Does the agency have a process for each of the following? (Select all that apply.)
- Ensuring that information collections include a Privacy Act Statement, if required
 - Receiving, processing, and responding to individuals' requests for access to and amendment of records in a system of records

Section 4: Systems of Records

- 4e. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information maintained in a system of records in order to ensure the following? (Select all that apply or indicate "N/A" if the agency does not maintain any Privacy Act systems of records)

N/A

Section 5: Considerations for Managing PII

- 5a. To what extent does the agency ensure that PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of is accurate, relevant, timely, and complete? (Select one of the following.)

Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

- 5b. To what extent does the agency limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions? (Select one of the following.)

Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

Section 6: Social Security Numbers

- 6a. Does the agency have an inventory of the agency's collection and use of Social Security numbers (SSNs)? (Indicate "N/A" if the agency does not collect, maintain, or use SSNs.)

Yes

- 6b. Does the agency maintain the inventory of SSNs as part of the agency's inventory of information systems referred to in question 2a? (Indicate "N/A" if the agency does not collect, maintain, or use SSNs, does not have an inventory of its collection, maintenance and use of SSNs, or does not maintain an inventory of information systems.)

Yes

- 6c. Has the agency developed and implemented a written policy to help ensure that any new collection or use of SSNs is necessary?

Yes

Section 6: Social Security Numbers

- 6d. Does the written policy referred to in question 6c provide specific criteria to use when determining whether the collection or use of SSNs is necessary? (Indicate "N/A" if the agency does not have a written policy.)
- Yes
- 6e. Does the written policy referred to in question 6c establish a process to ensure that any collection or use of SSNs determined to be necessary remains necessary over time? (Indicate "N/A" if the agency does not have a written policy.)
- Yes
- 6f. Has the agency taken steps during the reporting period to eliminate the unnecessary collection, maintenance, and use of SSNs? (Indicate "N/A" if the agency does not collect, maintain, or use SSNs, or if the agency has already eliminated all unnecessary collection, maintenance, and use of SSNs by the agency.)
- Yes

Section 7: Digital Services

- 7a. Does the agency maintain an inventory of the following? (Select all that apply or indicate "N/A" if the agency does not maintained an inventory of any digital services.)
- The agency's public websites
 - The agency's public applications (g., mobile applications, web applications)
 - The agency's public social media accounts
 - Other public-facing digital services used by the agency
- 7b. In accordance with the E-Government Act of 2002 and OMB guidance, does the agency maintain and post privacy policies on the following? (Select all that apply or indicate "N/A" if the agency does not maintain any of the following)
- The agency's public websites
 - The agency's public applications (g., mobile applications, web applications)
 - The agency's public social media pages and profiles
 - Other public-facing digital services used by the agency
- 7c. Does the agency have a process to regularly review and update the privacy policies for each of the following? (Select all that apply or indicate "N/A" if the agency does not maintained any of the following.)

Section 7: Digital Services

- The agency's public websites
- The agency's public applications (g., mobile applications, web applications)
- Other public-facing digital services used by the agency

7d. Has the agency developed and implemented a written policy for the agency's use of social media? (Indicate "N/A" if the agency does not use social media.)

Yes

7e. During the reporting period, did the agency use web management and customization technologies on any website or mobile application?

Yes

7f. During the reporting period, did the agency review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance? (Indicate "N/A" if the agency does not use web management and customization technologies.)

Yes

Section 8: Budget and Acquisition

8a. Does the agency identify and plan for the resources needed to implement the agency's privacy program?

Yes

8b. Does the agency have a policy that includes explicit criteria for analyzing privacy risks when considering IT investments?

Yes

8c. During the reporting period, did the agency review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, were explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

Yes

8d. To what extent does the agency plan and budget to upgrade, replace, or retire any information systems that maintain PII for which protections commensurate with risk cannot be effectively implemented?

Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

Section 8: Budget and Acquisition

- 8e. Does the agency ensure that, in a timely manner, the SAOP is made aware when information systems and components that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII cannot be appropriately protected or secured?

Yes

- 8f. Number of information systems and components used during the reporting period to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII that were reported to the SAOP because they cannot be appropriately protected or secured. (Indicate "N/A" if the SAOP is not made aware of information systems and components that cannot be appropriately protected or secured.)

0

Section 9: Contractors and Third Parties

- 9a. To what extent does the agency ensure that terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information incorporate privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information?

Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

- 9b. To what extent does the agency, consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function?

Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

- 9c. To what extent does the agency ensure appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information?

Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

- 9d. Does the agency maintain a mandatory agency-wide privacy awareness and training program for all contractors?

Yes

Section 9: Contractors and Third Parties

- 9e. Has the agency established rules of behavior, including consequences for violating rules of behavior, for contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?
- Yes
- 9f. Does the agency ensure that contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access (indicate "N/A" if the agency does not have established rules of behavior)?
- Yes

Section 10: Workforce Management

- 10a. Does the agency ensure that the agency's privacy workforce has the appropriate knowledge and skill?
- Yes
- 10b. Has the agency assessed its hiring, training, and professional development needs with respect to privacy during the reporting period?
- Yes
- 10c. Has the agency developed a workforce planning process to ensure that it accounts for privacy workforce needs?
- Yes
- 10d. Has the agency developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions?
- Yes

Section 11: Training and Accountability

- 11a. Does the agency maintain a mandatory agency-wide privacy awareness and training program for all Federal employees?
- Yes
- 11b. What percentage of Federal employees (including managers and senior executives) employed by the agency received foundational privacy training during the reporting period? (Indicate "N/A" if the agency did not collect this information for the reporting period.)

Section 11: Training and Accountability

100%

- 11c. Does the agency provide role-based privacy training to Federal employees with assigned privacy roles and responsibilities, including managers, before authorizing their access to Federal information or information systems?

Yes

- 11d. What percentage of Federal employees with assigned privacy roles received role-based training before being authorized to access Federal information or information systems? (Indicate "N/A" if the agency does not provide role-based privacy training.)

100%

- 11e. Has the agency ensured that measures are in place to test the knowledge level of information system users in conjunction with privacy training?

Yes

- 11f. To what extent does the agency ensure that all personnel are held accountable for complying with agency-wide privacy requirements and policies?

• Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

- 11g. Has the agency established rules of behavior, including consequences for violating rules of behavior, for Federal employees that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

Yes

- 11h. Does the agency ensure that Federal employees have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access? (Indicate "N/A" if the agency does not have established rules of behavior.)

Yes

Section 12: Incident Response

- 12a. Does the agency have a breach response plan that includes the agency's policies and procedures for each of the following? (Select all that apply or "N/A" if the agency does not have a breach response plan.)

Section 12: Incident Response

- Reporting a breach
- Investigating a breach
- Managing a breach

12b. Did the SAOP review the agency's breach response plan during the reporting period to ensure that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology? (Indicate "N/A" if the agency does not have a breach response plan.)

Yes

12c. Does the agency have a breach response team composed of agency officials designated by the head of the agency that can be convened to lead the agency's response to a breach?

Yes

12d. Did all members of the agency's breach response team participate in at least one tabletop exercise during the reporting period? (Indicate "N/A" if the agency does not have a breach response team.)

Yes

12e. How many breaches, as OMB Memorandum M-17-12 defines the term "breach," were reported within the agency during the reporting period?

0

12f. How many breaches, as OMB Memorandum M-17-12 defines the term "breach," did the agency report to the DHS Cybersecurity and Infrastructure Security Agency (CISA) during the reporting period?

0

12g. How many breaches, as OMB Memorandum M-17-12 defines the term "breach," did the agency report to Congress as major incidents (as defined in Fiscal Year 2021-2022 Guidance on Federal Security and Privacy Management Requirements) during the reporting period?

0

12h. What is the total number of individuals potentially affected by the breaches reported in question 12g? (Indicate "N/A" if the agency did not report a breach to Congress during the reporting period.)

N/A

Section 13: Risk Management Framework

- 13a. Has the agency implemented a risk management framework to guide and inform each of the following? (Select all that apply or "N/A" if the agency has not implemented a risk management framework.)
- Categorization of Federal information and information systems that process PII
 - Selection, implementation, and assessment of privacy controls
 - Authorization of information systems and common controls
 - Continuous monitoring of information systems that process PII
- 13b. Has the agency designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls?
- Yes
- 13c. Has the agency developed and maintained a written privacy continuous monitoring strategy?
- Yes
- 13d. Has the agency established and maintained an agency-wide privacy continuous monitoring program?
- Yes

Section 14: Privacy Program Website

- 14a. Does the agency have a Privacy Program Page located at (or redirected from) [www.[agency].gov/privacy|http://www.[agency].gov/privacy]?
- Yes
- 14b. Does the agency's Privacy Program Page include a list and provide links to complete, up-to-date versions of all agency SORNs? (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records.)
- Yes
- 14c. Does the agency's Privacy Program Page include a list and provide links to all PIAs? (Indicate "N/A" if the agency does not maintain, operate, or use any IT systems that require a PIA.)
- Yes

Section 14: Privacy Program Website

- 14d. Does the agency's Privacy Program Page include a list and provide links to up-to-date matching notices and agreements for all active matching programs in which the agency participates? (Indicate "N/A" if the agency does not participate in any matching programs.)
- Yes
- 14e. Does the agency's Privacy Program Page include citations and provide links to the final rules published in the Federal Register that promulgate each Privacy Act exemption claimed for their systems of records? (Indicate "N/A" if the agency has not claimed any Privacy Act exemptions for their systems of records.)
- Yes
- 14f. Does the agency's Privacy Program Page include a list and provide links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f)? (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records.)
- Yes
- 14g. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency policies on privacy, including any directives, instructions, handbooks, manuals, or other guidance?
- Yes
- 14h. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency reports on privacy?
- Yes
- 14i. Does the agency's Privacy Program Page include instructions in clear and plain language for individuals who wish to request access to or amendment of their records pursuant to 5 U.S.C. § 552a(d)? (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records.)
- Yes
- 14j. Does the agency's Privacy Program Page include appropriate agency contact information for individuals who wish to submit a privacy-related question or complaint?
- Yes
- 14k. Does the agency's Privacy Program Page identify the agency's SAOP and include appropriate contact information for his or her office? (Indicate "N/A" if the agency has not designated an SAOP.)
- Yes

Section 14: Privacy Program Website



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
Version 1.0	10/18/2021	Establishes HUD's Privacy Handbook.



Table of Contents

1.0 Introduction	6
1.1 Rescission	6
1.2 Applicability	6
1.2.1 Privacy Liaison Officers (PLOs).....	6
1.2.2 System Owners	6
1.3 Effective Date	7
 2.0 Personally Identifiable Information (PII) Handling Policies and Procedures.....	8
2.1 Definition of PII	8
2.2 Privacy Policy	8
2.2.1 Exclusions	9
2.2.2 Responsibility	9
2.2.3 PII Handling	9
2.2.4 PII Processing Requirements	10
2.2.5 Social Security Number Policy	13
2.2.6 SSN Inventory, Authorization, and Elimination	13
2.2.7 Acceptable Uses of SSNs	14
2.2.8 SSN Justification Memo	15
2.2.9 Legacy System Migration Plan	15
2.2.10 SSN Collection Forms	15
2.2.11 PII Protection at Workstations Policy.....	16
 3.0 Privacy Controls and Controls Assessment.....	16
3.1 Privacy Controls Inheritability	16
3.1.2 Organization-Level Privacy Controls	17
3.1.3 System-Level Privacy Controls.....	17
3.1.4 Hybrid Privacy Controls	17
 4.0 Privacy Act Requests.....	17
4.1 Identity Verification	18
4.2 Record Amendments and Appeals	18
4.2.1 Appeals Process	18
4.3 Amendment and Amendment Refusal Process.....	19
4.4 Disclosure Recordkeeping Policy	19
4.5 Disclosure Request Processing and Recordkeeping Guidance	20
4.6 Privacy Act Exceptions to Conditions of Disclosure	21
4.6.1 Most Commonly Used Privacy Act Exceptions.....	23
4.7 Privacy Act Exemptions.....	23
 5.0 Privacy Impact Assessments (PIA).....	24
5.1 PIA Template and Reference Guide.....	24
5.2 What Is a PIA?	24
5.3 Contents of a PIA	24



5.4 Is a PIA Required?	24
5.4.1 What Type of PIA Is Required?	25
5.4.2 Types of PIAs	25
5.4.3 PIAs – What Is a Significant Change?	25
5.4.4 Establishing or Modifying a PIA	26
5.5 PIA Review Schedule and Process	26
5.5.1 PIA Review Schedule	27
5.5.2 Annual PIA Review Process	27
5.5.3 Annual Certifications for Existing PIAs	28
5.6 PIA Website Publication	28
6.0 System of Records Notices (SORN)	29
6.1 SORN Templates and Reference Guide	29
6.2 What is a SORN?	29
6.3 Contents of a SORN:	29
6.4 Is a SORN Required?	30
6.5 What Type of SORN Is Required?	30
6.5.1 Types of SORNs	30
6.5.2 SORNs – What Is a Significant Change?	31
6.5.3 Reports and Additional Documents that Accompany SORNs	32
6.5.4 Establishing or Modifying a SORN	33
6.5.5 Rescinding a SORN	33
6.6 SORN Exemptions	34
7.0 Computer Matching Agreements (CMA)	34
7.1 What Is a CMA?	34
7.2 Contents of a CMA	35
7.3 Is a CMA Required?	35
7.4 What Type of CMA Is Required?	36
7.4.1 Types of CMAs	36
7.4.2 CMAs – What is a Significant Change?	37
7.4.3 Reports and Additional Documents for CMAs	37
7.5 CMA Procedures and Timing	38
7.6 Procedures for New and Significantly Modified CMAs	39
7.7 Procedures for Re-Establishment CMAs	41
7.8 Procedures for Renewal CMAs	42
7.9 CMA Review and Maintenance	43
7.10 CMA Website Publication	43
7.11 Data Integrity Board	43
7.11.1 DIB Responsibilities	43
7.11.2 DIB Membership	44
8.0 Federal Reporting Requirements	45
8.1 Annual Computer Matching Agreement (CMA) Activity Report	45
8.2 Annual SAOP FISMA Report	45
8.3 Annual SAOP FISMA Metrics	45



8.4 Annual SAOP FISMA Timeline.....	47
9.0 Forms and Contracts Requirements	48
9.1 Privacy Act Statements	48
9.2 Privacy Advisory Statements.....	49
9.3 Contracts.....	49
Appendix A. Authorities and References	54
Appendix B. Acronyms	55



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-01, which replaces and rescinds Privacy Act Handbook Version 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 8.0)
 - Social Security Number (SSN) Justification Memos and Reduction Plans (Section 2.2.8)
- 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 8.0)
- 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 [Date of Final Approval].

2.0 Personally Identifiable Information (PII) Handling Policies and Procedures

2.1 Definition of PII

Per the NIST 800-122, 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 National Institute of Standards and Technology (NIST) 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.

Other ways for communicating, sending, and receiving PII include:

- 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.



I. 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 2.3.2 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 can 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 Collection 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.

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 National Institute of Standards and Technology (NIST) 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 to respond 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:

Driver's license
U.S. Passport
Permanent Resident Card
Other state issued ID

List B:

Lease or proof of residence
Utility bill
Insurance letter

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](#).

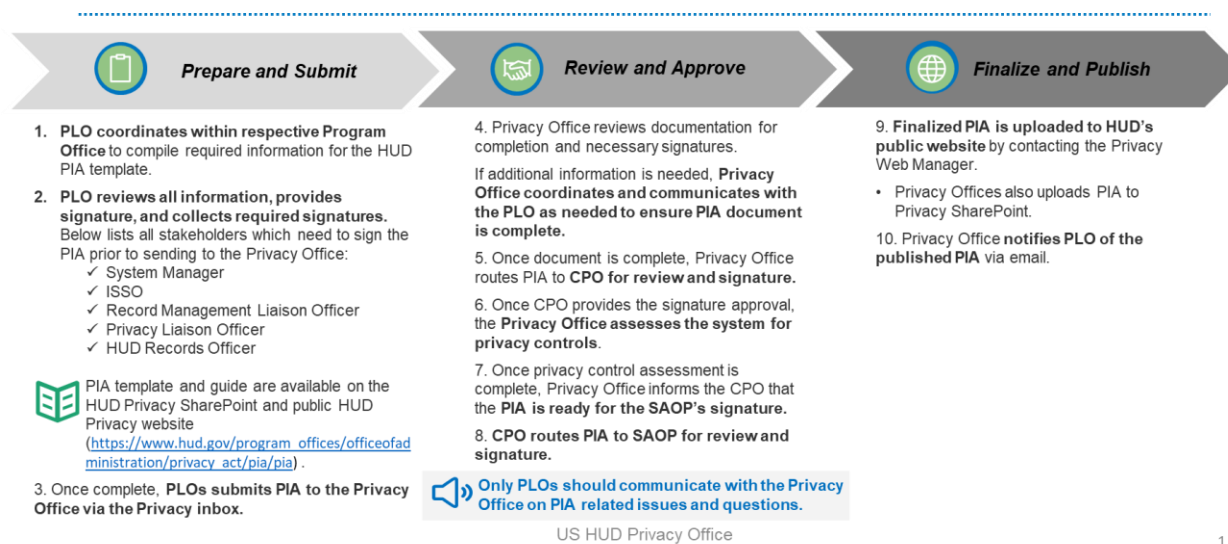


Diagram 1. PIA Workflow

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 and update 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. All necessary updates and changes must be submitted to the Privacy Office by June 30th. 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 Updated PIAs to confirm PIA accuracy. See Section 5.4 of this Handbook for details and instructions.	June 1 st
PLOs should conduct a status check for which Offices have and have not submitted Modified PIAs. PLOs should send submission reminders to System Owners who have not submitted their modified PIAs.	Not later than (NLT) June 15th
System Owners in each Office should complete reviewing PIAs and ensure Modified and Updated PIAs 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.

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 updated annual certification document to the Privacy Office.

5.5.3 Annual Certifications for Existing PIAs

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 PIA Certification.
5. **PLOs** submit the updated and signed PIA 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 Matchin 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.

- o 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 ◦ 2157 Rayburn House Office Building, Washington, DC 20515 • Senate Committee on Homeland Security and Governmental Affairs ◦ 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 ◦ 2157 Rayburn House Office Building, Washington, DC 20515 • Senate Committee on Homeland Security and Governmental Affairs ◦ 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 15 th of reporting year	Privacy Office
Draft internal schedule for collecting all required metrics and documentation and share with SAOP for approval	January 15 th 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:

- The authority (whether granted by statute or by Executive Order of the President) for soliciting the information and whether disclosure is mandatory or voluntary;
- The principal purpose(s) for which the information is intended to be used;
- The routine use(s) for which the information may be used, as published in the System of Records Notice (SORN),
- The effects on the individual, if any, of not providing all or any part of the requested information; and
- 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-123 - <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 1996" 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 OMB M-21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act
7. NIST, SP 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020 (includes updates as of Dec. 10, 2020)
8. NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)



Appendix B. Acronyms

Acronym	Definitions
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMA	Change Management Agreement
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
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

http://hudatwork.hud.gov/HUD/admin/Privacy_Home/



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	Updates HUD's Privacy Handbook and replaces Privacy Act Handbook (1325.1).



Table of Contents

1.0 Introduction	6
1.1 Rescission	6
1.2 Applicability	6
1.2.1 Privacy Liaison Officers (PLOs).....	6
1.2.2 System Owners	6
1.3 Effective Date	7
 2.0 Personally Identifiable Information (PII) Handling Policies and Procedures.....	8
2.1 Definition of PII	8
2.2 Privacy Policy	9
2.2.1 Exclusions	9
2.2.2 Responsibility	9
2.2.3 PII Handling.....	9
2.2.4 PII Processing Requirements	10
2.2.5 Social Security Number Policy	13
2.2.6 SSN Inventory, Authorization, and Elimination	13
2.2.7 Acceptable Uses of SSNs	14
2.2.8 SSN Justification Memo	15
2.2.9 Legacy System Migration Plan	15
2.2.10 SSN Collection Forms	16
2.2.11 PII Protection at Workstations Policy.....	16
 3.0 Privacy Controls and Controls Assessment.....	16
3.1 Privacy Controls Inheritability	17
3.1.2 Organization-Level Privacy Controls	17
3.1.3 System-Level Privacy Controls.....	17
3.1.4 Hybrid Privacy Controls	17
 4.0 Privacy Act Requests.....	18
4.1 Identity Verification	18
4.2 Record Amendments and Appeals	19
4.2.1 Appeals Process	19
4.3 Amendment and Amendment Refusal Process.....	20
4.4 Disclosure Recordkeeping Policy	20
4.5 Disclosure Request Processing and Recordkeeping Guidance	21
4.6 Privacy Act Exceptions to Conditions of Disclosure	22
4.6.1 Most Commonly Used Privacy Act Exceptions.....	23
4.7 Privacy Act Exemptions.....	23
 5.0 Privacy Impact Assessments (PIA).....	24
5.1 PIA Template and Reference Guide.....	24
5.2 What Is a PIA?	24
5.3 Contents of a PIA	24



5.4 Is a PIA Required?	24
5.4.1 What Type of PIA Is Required?	25
5.4.2 Types of PIAs	25
5.4.3 PIAs – What Is a Significant Change?	25
5.4.4 Establishing or Modifying a PIA	26
5.5 PIA Review Schedule and Process	27
5.5.1 PIA Review Schedule	27
5.5.2 Annual PIA Review Process	27
5.5.3 Annual Certifications for Existing PIAs	28
5.6 PIA Website Publication	28
6.0 System of Records Notices (SORN)	29
6.1 SORN Templates and Reference Guide	29
6.2 What is a SORN?	29
6.3 Contents of a SORN:	29
6.4 Is a SORN Required?	30
6.5 What Type of SORN Is Required?	30
6.5.1 Types of SORNs	30
6.5.2 SORNs – What Is a Significant Change?	31
6.5.3 Reports and Additional Documents that Accompany SORNs	32
6.5.4 Establishing or Modifying a SORN	33
6.5.5 Rescinding a SORN	33
6.6 SORN Exemptions	34
7.0 Computer Matching Agreements (CMA)	34
7.1 What Is a CMA?	34
7.2 Contents of a CMA	35
7.3 Is a CMA Required?	36
7.4 What Type of CMA Is Required?	36
7.4.1 Types of CMAs	36
7.4.2 CMAs – What is a Significant Change?	37
7.4.3 Reports and Additional Documents for CMAs	37
7.5 CMA Procedures and Timing	38
7.6 Procedures for New and Significantly Modified CMAs	39
7.7 Procedures for Re-Establishment CMAs	41
7.8 Procedures for Renewal CMAs	42
7.9 CMA Review and Maintenance	43
7.10 CMA Website Publication	43
7.11 Data Integrity Board	43
7.11.1 DIB Responsibilities	43
7.11.2 DIB Membership	44
8.0 Federal Reporting Requirements	45
8.1 Annual Computer Matching Agreement (CMA) Activity Report	45
8.2 Annual SAOP FISMA Report	45
8.3 Annual SAOP FISMA Metrics	45



8.4 Annual SAOP FISMA Timeline.....	47
9.0 Forms and Contracts Requirements	48
9.1 Privacy Act Statements	48
9.2 Privacy Advisory Statements.....	49
9.3 Contracts.....	49
Appendix A. Authorities and References.....	54
Appendix B. Acronyms.....	55



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-01, which replaces and rescinds Privacy Act Handbook Version 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.

I. 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 Collection 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:

Driver's license
U.S. Passport
Permanent Resident Card
Other state issued ID

List B:

Lease or proof of residence
Utility bill
Insurance letter

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 HUDFOIAppeals@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: HUDFOIAppeals@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](#).

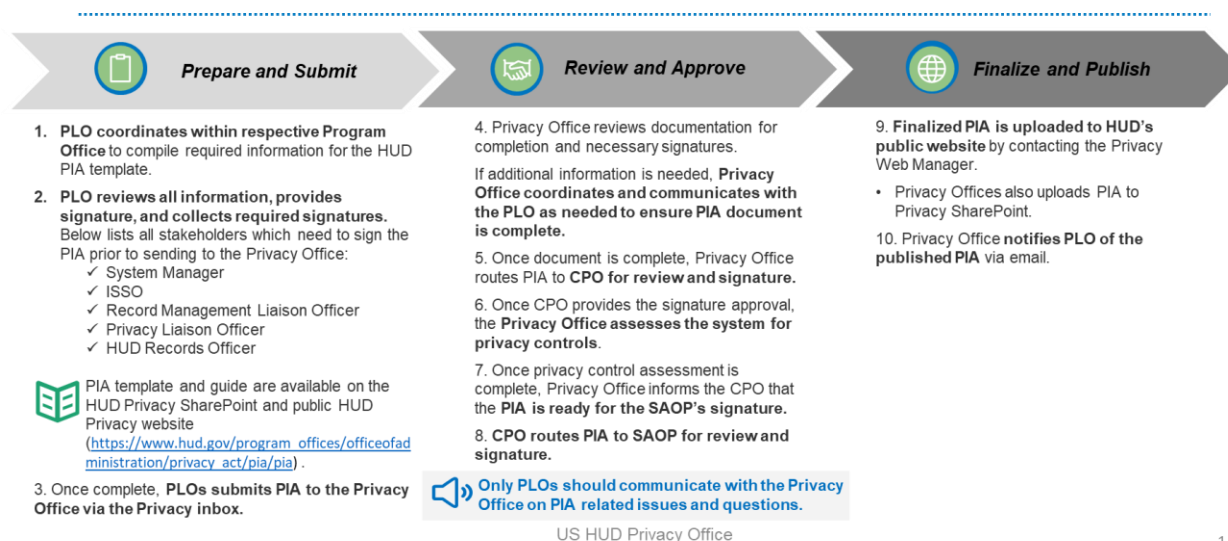


Diagram 1. PIA Workflow



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 1 st
PLOs should conduct a status check for which Offices have and have not submitted Modified PIAs and or Annual PIA Certifications. PLOs 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 ◦ 2157 Rayburn House Office Building, Washington, DC 20515 • Senate Committee on Homeland Security and Governmental Affairs ◦ 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 ◦ 2157 Rayburn House Office Building, Washington, DC 20515 • Senate Committee on Homeland Security and Governmental Affairs ◦ 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 15 th of reporting year	Privacy Office
Draft internal schedule for collecting all required metrics and documentation and share with SAOP for approval	January 15 th 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:

- The authority (whether granted by statute or by Executive Order of the President) for soliciting the information and whether disclosure is mandatory or voluntary;
- The principal purpose(s) for which the information is intended to be used;
- The routine use(s) for which the information may be used, as published in the System of Records Notice (SORN),
- The effects on the individual, if any, of not providing all or any part of the requested information; and
- 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-123 - <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 1996" 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 OMB M-21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act
7. NIST, SP 800-53 Revision 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)



Appendix B. Acronyms

Acronym	Definitions
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMA	Change Management Agreement
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

The U.S. Department of Housing and Urban Development (HUD)



PRIVACY PROGRAM PLAN

OCTOBER 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.**

Table of Contents

1.0 Introduction.....	3
1.1 Annual Update	3
2.0 Overview of HUD Privacy Program	3
2.1 Mission Statement.....	3
2.2 HUD Privacy Office Organization	4
2.3 Strategic Goals and Objectives for Privacy	5
3.0 Privacy Workforce Management	7
4.0 Budget and Acquisition	7
5.0 Risk Management Framework.....	8
6.0 Privacy Control Requirements	8
6.1 HUD Control Allocation	9
6.2 Privacy Impact Assessment (PIA).....	9
6.3 Contractors and Third Parties	10
6.4 System of Records Notices (SORN)	11
6.5 Privacy Act Statements	11
6.6 Privacy Act Regulations	11
7.0 Privacy Policy	12
8.0 Breach Response and Management.....	12
9.0 Awareness and Training	13
9.1 New Employee Orientation Training.....	13
9.2 HUD Virtual University (HVV)	13
9.3 Role-Based Training	13
10.0 Privacy Reporting.....	13
11.0 Conclusion.....	14

1.0 Introduction

The purpose of the HUD Privacy Program Plan is to provide an overview of HUD's Privacy Program. This Plan, which is consistent with the requirements enumerated in OMB Circular A-130, *Managing Information as a Strategic Resource* includes:

- A description of the structure of HUD's Privacy Program;
- The resources dedicated to HUD's Privacy Program;
- The role of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer (CPO), and other privacy staff;
- The strategic goals and objectives of the Privacy Program;
- The program management controls in place to meet applicable privacy requirements and manage privacy risks; and
- Additional information deemed important by HUD's SAOP to provide an overview of HUD's Privacy Program requirements.

1.1 Annual Update

The Privacy Program Plan will be reviewed at minimum on an annual basis to ensure program objectives align with the most current Federal requirements.

2.0 Overview of HUD Privacy Program

2.1 Mission Statement

HUD's program is led by HUD's SAOP and is managed by the CPO within the Privacy Office, located in HUD's Office of the Assistant Secretary for Administration, Chief Administrative Officer (OCAO). The mission of the HUD Privacy Program is to protect and minimize impacts on the privacy of individuals, while achieving HUD's mission.

The Office plans to achieve this mission by cultivating a strong culture of privacy protection throughout the Department and providing a risk-based, enterprise-wide program based upon sound privacy practices in compliance with applicable laws and that maintains and builds public trust. The Privacy Office implements requirements in the Privacy Act of 1974, *as amended*; E-Government Act of 2002; and the Federal Information Security Modernization Act (FISMA), as well as policy directives and best practices issued in furtherance of those Acts.

The Privacy Office adheres to HUD's Privacy Policy and the policy framework embodied in the Fair Information Practice Principle (FIPPs) to ensure that individual privacy is protected throughout the creation, collection, maintenance, use, dissemination and disposal of all personally identifiable information (PII) maintained by the HUD. The Privacy Office carries out the following core functions:

- Develops and administers HUD's privacy policies and procedures;

- Provides privacy awareness training and targeted privacy trainings to HUD personnel;
- Assesses all new or proposed programs, systems, technologies, and business processes for privacy risks and provides recommendations to strengthen privacy protections;
- Collaborates with HUD's Office of Information Technology Security (OITS) to implement and operationalize policies and tools to secure the confidentiality, integrity, and availability of HUD's information and information systems;
- Operates a data breach response program to ensure that all incidents involving personally identifiable information (PII) are properly reported, investigated, and mitigated, as appropriate; and
- Maintains updated privacy artifacts in compliance with legal requirements (e.g., System of Records Notice, Privacy Impact Assessments, and Privacy Act Notices).

2.2 HUD Privacy Office Organization

HUD's Privacy Program is housed within the Office of the CAO. The Privacy Office develops and executes policies and procedures to ensure that privacy is protected for all employees, contractors and those who entrust their personal information to the HUD. The Privacy Office is led by HUD's SAOP pursuant to OMB Memorandum 16-24, *Role and Designation of Senior Agency Officials for Privacy*.

The SAOP is HUD's key policy advisor on implementing the HUD's Privacy Policy, Privacy Act of 1974; the privacy provisions of the Federal Information Security Modernization Act (FISMA); the privacy provisions contained in the E-Government Act of 2002; Office of Management and Budget (OMB) requirements; and National Institute of Standards and Technology (NIST) guidance. In accordance with OMB Circular A-130, *Managing Information as a Strategic Resource*, the SAOP is responsible for:

- Serving as HUD's senior policy authority on matters relating to the public disclosure of information, advising on privacy issues related to informed consent, disclosure risks, and data sharing;
- Developing and overseeing implementation of Agency-wide policies and procedures relating to the Privacy Act, and assuring that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- Communicating HUD's privacy vision, principles, and policies internally and externally working with the Privacy Liaison Officers (PLO's) in each business area as appropriate;
- Advocating strategies for data and information collection and dissemination, and conducting an annual PII inventory to ensure HUD's privacy policies and principles are reflected in all operations;

- Managing privacy risks associated with HUD activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems.
- Ensuring that HUD employees have the appropriate training and education concerning privacy laws, regulations, policies, and procedures;
- Working with HUD stakeholders to ensure the vendors with access to PII that engage in business with HUD abide by federal privacy requirements;
- Overseeing HUD's process for reviewing and approving Privacy Impact Assessments (PIA) to ensure compliance with the E-Government Act;
- Coordinating with HUD's Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) to ensure that the FISMA authorization and accreditation (A&A) process for new and existing systems appropriately addresses privacy-related risks;
- Partnering with the CTO and CISO to ensure all aspects of HUD's Privacy Program are incorporated into HUD's enterprise infrastructure, information technology (IT), and IT security program.

In accordance with OMB Memorandum 16-24, HUD's SAOP has delegated the daily operations of HUD's Privacy Program to HUD's CPO. With the oversight of HUD's SAOP, the CPO handles all the substantive components of HUD's Privacy Office. HUD's Privacy Office is staffed by a team of management analysts and specialists who have privacy duties. Additionally, each business area is required to appoint a Privacy Liaison Officer who serves as the ambassador between the agency's office and the Privacy Office. The PLO is responsible for overseeing compliance with privacy regulations in their respective business area, including understanding PIAs, SORNs, CMAs, breach notification guidelines, and other requirements for handling PII.

2.3 Strategic Goals and Objectives for Privacy

GOAL 1

Maintain compliance with federal privacy laws, regulations, and best practices.

The Privacy Office

- Objective 1.1 – Increase accountability and transparency by enhancing and regularly updating HUD's foundational privacy documents to comply with the Privacy Act, the E-Government Act of 2002, OMB requirements, and best practices. These documents include HUD's SORNs, and PIAs.
- Objective 1.2 – Provide sound and consistent legal advice to HUD's client offices concerning the interpretation and application of federal privacy laws, regulations, and other best practices.

- Objective 1.3 – Review, assess, and advise business owners throughout HUD about HUD programs, projects, information sharing arrangements, systems, and other initiatives to comply with the HUD Privacy Policy. This includes limiting the collection, maintenance, use, and dissemination of PII whenever possible.
- Objective 1.4 – Ensure that privacy-related complaints and incidents at HUD are reported systematically, efficiently processed, and appropriately mitigated in accordance with legal requirements and HUD policies and procedures.

GOAL 2

Foster a culture of privacy and demonstrate leadership through policy and strategic partnership

The Privacy Office's core mission is to preserve and enhance privacy protections for all individuals who entrust their personal information to the Agency and fostering a culture of privacy at the Agency is a necessary component for achieving this mission. In accordance with the FIPPs, HUD is authorized to only collect information necessary to carry out its mission and must use that information in accordance with the stated purpose for which it was originally collected. HUD is also authorized to collect, maintain, use, and disseminate personal information from individuals who work and seek to work for the Agency.

- Objective 2.1 – Provide guidance and issue policies related to privacy by partnering with the PLO's and leaders across HUD to embed and enhance privacy protections throughout the life cycle of HUD initiatives, programs, projects, and systems.
- Objective 2.2 – Leverage the expertise of the Federal Privacy Council, as well as experts from professional privacy associations, to foster dialogue and learn about emerging issues.
- Objective 2.3 – Understand the PII collected from each business area by collecting information from the annual PII inventory.
- Objective 2.4 – Partner with the CIO and CISO on key initiatives that promote privacy, including embedding privacy in the development lifecycle.

GOAL 3

Provide outreach, training, and education to promote and enhance privacy Agency-wide

HUD's Privacy Office ensures that all HUD personnel have a baseline understanding of federal privacy requirements by providing training for new hires and annually thereafter. HUD's Privacy Office also develops and provides targeted, role-based training to employees with specialized roles on a periodic basis.

- Objective 3.1 – Ensure consistent application of privacy requirements across the Agency.
- Objective 3.2 – Develop and deliver targeted, role-based training for employees with specialized roles and other key stakeholders across the Agency.
- Objective 3.3 – Provide privacy awareness as laid out in the communication plan by educating HUD personnel about the importance of adhering to the FIPPs and partner with the PLOs to embed privacy into HUD’s business practices.

GOAL 4

Develop and maintain top privacy professionals that can serve as trusted privacy advisors for the Agency

HUD’s Privacy Office has grown considerably over the past few years and continues to mature. Attracting and retaining specialized talent is critical to the Privacy Office’s continued success. Providing support, opportunities for professional growth and development, and maintaining a workplace environment in which they are valued are all crucial to recruiting and maintaining a high-performing workforce.

- Objective 4.1 – Support employee development and emphasize the importance of training and professional development in performance planning, including increasing the number of individuals with privacy certifications through a nationally recognized association each year.
- Objective 4.2 – Provide advice and guidance to HUD offices on complicated privacy issues.

3.0 Privacy Workforce Management

HUD’s SAOP collaborates with members of HUD’s executive leaders to maintain and enhance a current workforce planning process, maintain workforce skills, recruit and retain privacy professionals, and to develop a set of competency requirements for staff in HUD’s Privacy Office. HUD’s SAOP facilitates and oversees role-based training for HUD’s workforce to ensure HUD personnel have the appropriate knowledge and skill to embed privacy into their respective business processes. Finally, HUD’s SAOP collaborates with members of HUD’s executive leaders to ensure that managers take advantage of flexible hiring authorities for specialized positions where necessary.

4.0 Budget and Acquisition

HUD’s SAOP ensures that the Agency identifies and plans for the resources needed to implement its Privacy Program each year. The SAOP collaborates with



members of HUD's ELC to review IT capital investment plans and budgetary requests to ensure that privacy requirements and associated privacy controls are identified and collaborates with key stakeholders to ensure privacy risks are addressed to the maximum extent possible.

5.0 Risk Management Framework

HUD adheres to the process described in NIST SP 800-37, *Risk Management Framework Rev. 5*, to incorporate information security and privacy risk management activities into the system development life cycle. The SAOP collaborates with HUD's CTO and CISO to:

- Analyze data elements used by each of HUD's information system, including the information processed, maintained, and transmitted by each system, based on an impact analysis compliant with NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; and
- Conduct a privacy impact assessment which assesses the privacy risks for each of HUD's information systems.

Additionally, HUD maintains a Security and Privacy Control Catalogue, a living document that addresses all security and privacy requirements listed in NIST SP 800-37 Rev. 5. The catalogue's privacy controls include (1) privacy authorizations policy and procedures, (2) authority to collect, (3) purpose specification, and (4) information sharing with external parties.

6.0 Privacy Control Requirements

HUD has implemented NIST SP 800-53, Rev. 4 to ensure compliance with applicable statutory, regulatory, and policy requirements with respect to information security. The Privacy Office is in the process of finalizing privacy controls for HUD's information systems in compliance with NIST SP 800-53, Rev. 4 Appendix J. HUD also adheres to Section 208 of the E-Government Act of 2002, which requires agencies to conduct PIA for electronic systems and collections. The Privacy Office conducted an initial analysis, known as a privacy threshold analysis (PTA) of each of HUD's electronic systems to determine whether a PIA is required. HUD determined that it was unnecessary to separately conduct PTAs as the initial analysis could be streamlined and incorporated into the PIA. Finally, HUD ensures compliance with the Privacy Act by publishing SORNs in the Federal Register.

6.1 HUD Control Allocation

HUD's Privacy Office is in the process of finalizing its baseline privacy controls document, which implements the requirements contained in NIST SP 800-53, Rev. 4 Appendix J. The Privacy Office will designate each control as program management, common, information system-specific, or hybrid. Common controls are controls that are inherited by multiple information systems. Information system-specific controls are controls that are implemented for a particular information system or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system in part as a common control and in part as an information system-specific control. The determination as to whether a privacy control is a common, information system-specific, or hybrid control is based on context..

6.2 Privacy Impact Assessment (PIA)

A PIA is legally required by Section 208 of the E-Government Act of 2002 and analyzes how information in an identifiable form is collected, maintained, stored, and disseminated. The PIA analyzes the privacy risks as well as the protections and process for handling information to mitigate the privacy risks. PIAs are conducted when:

1. Developing or procuring information systems or projects that collect, maintain, or disseminate information in identifiable form, from or about, members of the public; or
2. Initiating a new electronic collection of information in identifiable form from 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

HUD has incorporated the FIPPS into its PIAs. HUD's PIAs describe: (1) the legal authority that permits the collection of information; (2) the specific type of information used by the system; (3) how and why the system uses the information; (4) whether the system provides notice to individuals that their information is used by the system; (5) the length of time the system retains information; (6) whether and with whom the system disseminates information; (7) procedures individuals may use to access or amend information used by the system; and (8) physical, technical, and administrative safeguards applied to the system to secure the information.

Pursuant to HUD's PTA/PIA Policy and Procedures, if the SAOP determines a PIA is required, the Information System Security Officer (ISSO) and System Owner (SO) complete the PIA. A Privacy Analyst in the Privacy Office then reviews the PIA to ensure it is accurate and complete and analyze whether

privacy risks are mitigated to an acceptable level. Once complete, the SAOP signs the document.

PIAs should be updated when a new authorization to operate date has been issued, at minimum every three years or as necessary where a system change creates new privacy risks. Examples include:

1. Conversions – Converting paper-based records to electronic systems;
2. Anonymity to Non-Anonymous – Applying functions to an existing information that changes anonymous information into information in identifiable form;
3. Significant System Management Changes – Applying new technologies that significantly change how information in identifiable form is managed in the system
4. Significant Merging – Adopting or altering business processes so government databases holding information in identifiable form are merged, centralized, or matched with other databases or otherwise significantly manipulated;
5. New Public Access – Applying new user authenticating technology (e.g., password, digital certificate, biometric) to electronic information accessed by the public;
6. Commercial Sources – Incorporating information in identifiable form purchased or obtained from public or commercial sources into existing databases;
7. New Interagency Uses – Working together with other agencies on shared functions involving significant new uses or exchanges of information in identifiable form;
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
9. Alterations in the Character of Data – When the nature of new information in identifiable form added to a collection raises the risks to personal privacy (e.g., addition of health or financial information).

6.3 Contractors and Third Parties

HUD ensures contractors and third parties that: (1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the Agency; or (2) operate or use information systems on behalf of the Agency comply with the mandated privacy requirements. HUD's Privacy Office coordinates with HUD's Contracting Division to ensure that the applicable privacy clauses are included in the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of HUD information.

6.4 System of Records Notices (SORN)

HUD adheres to Privacy Act requirements for publishing SORNs in the Federal Register. A system of records is a group of any records under the control of any agency 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.

The Privacy Act incorporates the FIPPs into SORNs. SORNs: (1) inform HUD's many clients and partners about the kinds of personal information agencies maintain; (2) state the legal authority under which the agency collects and maintains individuals' information; (3) describe the purpose for which the agency may use the information; (4) describe the categories of information contained in the system of records; (5) describe the physical, administrative, and technical safeguards used to secure the information; (6) describe how an individual may request access to or amend their information; and (7) describe with whom the agency may share information contained within the system of records without obtaining prior consent of the data subject.

6.5 Privacy Act Statements

Privacy works with each of the Program Offices to ensure that a Privacy Act statement is provided or otherwise made available when the Agency collects PII. HUD's Privacy Act Statements have incorporated key aspects of the FIPPs and provide individuals with the:

- Agency's legal authority to collect the information, such as statute, executive order, and/or regulation;
- Purpose for collecting the information and how it will be used;
- Routine uses of the information, which describes to whom HUD may disclose information and for what purpose; and
- Whether providing the information is mandatory or voluntary, along with the effects if any, on the individual for not providing all or any part of the information requested.
- Applicable SORN and link

6.6 Privacy Act Regulations

HUD has promulgated regulations which implement the requirements contained in the Privacy Act of 1974. The regulations, which are located at 5 C.F.R. Part 1630, apply to all records maintained by HUD that contain identifiable information about individuals and which are included as part of a system of records. HUD's regulations establish procedures that enable individuals to access records maintained about them; provide detailed procedures for how to amend inaccurate information; and limit individuals who may access such information.



7.0 Privacy Policy

HUD has developed a [privacy policy](#) that establishes a set of privacy principles and applies those principles to employees, individuals applying for HUD programs, business partners, contractors and clients. These principles and policy requirements govern how HUD identifies, processes, and minimizes PII and explains how HUD complies with the privacy requirements.

HUD will be accountable for complying with these principles, providing training to personnel who use or process PII, and auditing the actual use of PII to demonstrate compliance with these principles and applicable privacy protection requirements. Additionally, HUD will incorporate key privacy requirements into the Agency's Rules of Behavior.

8.0 Breach Response and Management

HUD has an obligation to protect the information entrusted to the Agency. The Privacy Office takes this obligation very seriously and has developed a policy and procedures to inform HUD employees and contractors of their obligation to protect PII and to instruct them specific steps they must take in the event there is an actual or potential compromise of PII. HUD's process for responding to a breach of PII are part of the Agency's formal Incident Response Policy and Procedures and is based on OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* and requires:¹

- All HUD employees and contractors to immediately report any potential or actual incidents to HUD's Computer Incident Response Team (CIRT) as soon as they become aware that an incident may have occurred;
- The CIRT investigates the facts and circumstances surrounding the potential incident and further requires the SAOP and CPO or their designee to investigate whether PII was potentially or actually compromised;
- The SAOP determines which remediation methods should be used in the event of an actual compromise of PII based on the type of harm caused to the individual(s);
- The CIRT conducts after action reports for high- and moderate-risk incidents that document the details of the incidents and the steps taken to remediate the gaps that caused the incident to occur; and
- The SAOP shall periodically, but not less than annually, convene the agency's breach response team to hold a tabletop exercise. The purpose of the tabletop exercise is to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand their specific roles.

¹ HUD's Privacy Office works closely with the CISO and his team to uphold the confidentiality, integrity, and availability for HUD information and information systems. These procedures describe the Privacy Office's role in the incident response process. In accordance with HUD's Incident Response Policy and Procedures, there are additional steps the CISO is required to take to detect, contain, respond to, and prevent incidents, in accordance with NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*¹

9.0 Awareness and Training

HUD requires all employees and contractors to complete the General Cybersecurity Training when first beginning work with the Agency and annually thereafter. HUD conducts its annual training through the Agency's HUD Virtual University (HVVU). The training provides an overview of important statutory, regulatory, and other federal privacy requirements, including the Privacy Act and the E-Government Act of 2002. For those with privacy specific responsibilities in PII handling, there are additional role-based trainings. The Privacy Office has also created a communication plan for developing and executing communications across HUD.

9.1 New Employee Orientation Training

HUD's Privacy Office provides general cybersecurity training to all new employees on their first day of beginning work with the Agency. New employee orientation sessions provide an overview about the importance of privacy at HUD, how to handle privacy-protected information, and the penalties for violating the Privacy Act. This presentation also includes an overview of the importance of completing and PIAs for all HUD systems. Finally, the Privacy Office ensures all new employees are briefed on the importance of immediately reporting all potential and actual incidents involving PII to the IRT. All employees will have access to privacy training materials through their PLO.

9.2 HUD Virtual University (HVVU)

HUD delivers annual privacy training, through the Agency's centralized training system, called HUD Virtual University. Employees and contractors can access content contained in the system. A list of privacy trainings available at HVVU can be found in the Privacy Training Plan located on the Privacy Office sharepoint.

9.3 Role-Based Training

In addition to new-hire and annual privacy training requirements, HUD's Privacy Office provides role-based training to employees with specialized roles on a periodic basis, focusing on how employees in various HUD Offices should leverage the federal guidelines and best practices as part of their official duties. PLOs in every HUD Office will have additional monthly trainings for their role.

10.0 Privacy Reporting

The Federal Information Security Modernization Act (FISMA) requires federal agencies to develop, document, and implement agency-wide information security programs that include plans and procedures to ensure the security of operations for information systems that support the operations of the agencies. All federal agencies are required to submit an annual report to OMB; the United States Department of Homeland Security; and to specific Committees in the United States Representatives and Senate. HUD's SAOP completes the SAOP report, which is submitted as part of HUD's annual FISMA report. In response to questions developed by DHS and OMB, HUD's SAOP



provides an overview of a variety of activities conducted by the Privacy Office during the reporting period.

As a part of its privacy plan, HUD has created a Privacy Office Executive Dashboard, a bimonthly report with updates on Privacy Office highlights, information on incidents, risks and issues, as well as updates on communications, trainings, consults, and PII minimization efforts.

11.0 Conclusion

HUD is committed to safeguarding PII the information entrusted to the Agency. HUD's Privacy Office uses all methods of regulation, policy, guidance, and principles to further it is objective across the Agency. Privacy considerations are embedded in all levels of decision-making and operations in an effort to continue to build a culture of trust and privacy at the HUD.

Nancy Corsiglia

Senior Agency Official for Privacy

October 2021



HUD Privacy Program Changes FY21

In FY21, HUD was able to significantly mature its Privacy Program through improvements to policy, Personally Identifiable Information (PII) identification and minimization, communications, and training.

- HUD updated its Privacy Handbook, which establishes policies, procedures, requirements, and guidelines for the implementation of HUD's Privacy responsibilities. These requirements include PII handling policies and procedures, information disclosure and accounting, risk assessments, data use inventorying and recordkeeping, Federal reporting, and forms and contracts requirements.
 - The Handbook establishes HUD's Social Security Number collection policies, including collection and use limitation, purpose justification, and use of alternative identifiers whenever possible.
- The Privacy Office advanced PII identification and minimization efforts by issuing data calls and coordinating with stakeholders across the Department to complete system privacy documentation.
 - As a part of this effort, the Privacy Office has published reference guides, templates, and other supplemental material to support compliance privacy documentation across Program Offices.
- The Privacy Office has continued to hold recurring communications and trainings with Privacy Liaison Officers (PLOs) and System Owners, allowing for improved communication and workflow. HUD is continuing to develop privacy role-based trainings to improve the overall privacy compliance and awareness across the organization.

The U.S. Department of Housing and Urban Development (HUD)



HUD Breach Notification Response Plan (HBNRP) 3150.1 REV 1.0

10/16/2021

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	10/16/2021	Establishes a detailed procedure of privacy incident and breach response plans. This revision replaces both the <i>Office of the Chief Information Office (OCIO) Handbook 3150.1 Breach Notification Policy and Response Plan</i> and <i>HUD Breach Notification Response Team - Privacy Breach Standard Operating Procedures, 3150.2</i> .



Table of Contents

Document Change History	2
1.0 Introduction	6
1.1 Rescission	6
1.2 Scope	6
1.3 Effective Date	7
2.0 Definitions	7
2.1 System of Records	7
2.2 Personally Identifiable Information	7
2.3 Sensitive Personally Identifiable Information	7
2.4 Security vs. Privacy Incidents.....	8
2.5 Breach	9
2.6 Notice	9
2.7 Harm	9
3.0 Privacy Incident Handling Roles and Responsibilities	10
3.1 HUD Breach Notification Response Team	10
3.2 General Responsibilities of Each Member	10
3.3 Specific Responsibilities of Each Member	11
3.3.1 Senior Agency Official for Privacy	11
3.3.2 Chief Privacy Officer	11
3.3.3 Chief Information Security Officer.....	12
3.3.4 Assistant Secretary for Congressional and Intergovernmental Relations....	12
3.3.5 Associate Chief Information Officer for Information Assurance	12
3.3.6 Chief Financial Officer (CFO)	13
3.3.7 Chief Information Officer.....	13
3.3.8 Chief Procurement Officer	13
3.3.9 Customer Relationship Manager	14
3.3.10 General Counsel	14
3.3.11 General Deputy Assistant Secretary for Public Affairs	14
3.3.12 Human Capital Officer	14
3.3.13 Inspector General	15
3.3.14 Affected Program Manager	15
3.3.15 Affected Office Manager.....	16
3.3.16 Senior Advisor to the Secretary.....	16
3.4 Other Individuals and Entities.....	16
3.4.1 Deputy Secretary.....	16
3.4.2 Chief Operating Officer.....	17
3.4.3 Deputy Chief Information Officer	17
3.4.4 HUD Computer Incident Response Team (HUD SOC/CIRT)	17
3.4.5 HUD Help Desk	17
3.4.6 HUD Personnel	17
3.4.7 Associate CIO for Service Delivery	18



3.4.8 HUD Third Parties	18
5.0 Privacy Incident Response Process	18
5.1 Incident Detection and Reporting	18
5.1.1 Initial Discovery and Reporting Procedures.....	18
5.1.2 Incident Processing	19
5.1.3 Incident Ticket Content.....	20
6.0 Preliminary Investigation, Risk Analysis, and Escalation	21
6.1 Preliminary Investigation	21
6.1.1 Identity Theft Assessment	22
6.2 Impact Level Determination and Procedures.....	23
7.0 Full Risk Assessment	25
7.1 Incident Classification.....	25
7.2 PII Confidentiality Impact Levels	26
7.2.1 PII Confidentiality Impact Factors.....	27
7.3 Investigation Method	30
7.3.1 Investigators' Plan of Action	30
8.0. Notification.....	31
8.1 Congressional Notification	31
8.2 Notification of Individuals.....	32
8.3 Determine Source of Individual Notification.....	33
8.4 Create Content for Individual Notification	35
8.5 Determine Means of Individual Notification	37
8.6 Coordinate Internally	38
8.7 Determine Need for Third Party Notification	38
8.8 Provide Notification	39
9.0. Mitigation	40
9.1 Purpose of Mitigation.....	40
9.2 Timing and Sequence	40
9.3 Mitigation Responsibilities	40
9.4 Incident Containment	41
9.5 Countermeasures to Minimize Harm	42
9.5.1 Ordering Credit Monitoring	43
9.6 Breach Involving a Disruption of Services to Information System or Data Store	43
9.7 Compromises of Paper-Based Systems.....	44
10.0 Closure.....	44
11.0 Supplemental Activities	44
11.1 Activities	44
11.1.1 Lessons Learned.....	45



11.1.2 Using Collected Incident Data	46
Appendix A. Illustrations of Privacy Incidents	47
Insufficient Notice	47
Insufficient Redress.....	47
Loss of Control	48
Compromise	48
Unauthorized Disclosure	48
Unauthorized Acquisition.....	49
Unauthorized Access (Internal and External)	49
Appendix B. Sample Notification Letter	50
Appendix C. Press Release	52
Appendix E. Roles and Responsibilities Checklists.....	53
CPO Roles and Responsibilities Checklist	53
Chief Information Security Officer (CISO) Roles and Responsibilities Checklist ..	58
Senior Agency Official for Privacy Roles and Responsibilities Checklist.....	62
Chief Information Officer Roles and Responsibilities Checklist	63
Chief Financial Officer Roles and Responsibilities Checklist.....	65
Chief Procurement Officer Roles and Responsibilities Checklist	65
General Counsel Roles and Responsibilities Checklist	68
Inspector General Roles and Responsibilities Checklist	69
Program Manager Roles and Responsibilities Checklist.....	71
HUD Personnel Roles and Responsibilities Checklist	72
Customer Relationship Manager Roles and Responsibilities Checklist.....	73
General Deputy Assistant Secretary for Public Affairs Roles and Responsibilities Checklist	75
Human Capital Officer Roles and Responsibilities Checklist.....	77
Appendix F. Acronyms	78
Appendix G. List of References	79



1.0 Introduction

The HBNRP outlines HUD's approach for coordinating a response to a privacy incident. This document complies with Office of Management and Budget (OMB) Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information", January 3, 2017, which requires all individuals with access to the agency's Federal information and information systems to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and procedures, National Institute of Standards and Technology (NIST) standards and guidelines, as well as the United States Computer Emergency Readiness Team (US-CERT) notification guidelines.

Safeeguarding privacy is intrinsic to the nature of HUD's mission. Without strong adherence to federally required protection of personally identifiable information, the public will not trust that HUD can maintain the sensitive personal data required by federal affordable housing programs and FHA insured mortgages. Loss of trust could impede HUD's ability to provide services to those who need them most. HUD is committed to the privacy of its customers and expects compliance with these Standard Operating Procedures (SOP) to maintain and increase public trust.

1.1 Rescission

This document rescinds and replaces the following:

- Office of the Chief Information Office (OCIO) Handbook 3150.1, Breach Notification Policy and Response Plan.
- HUD Breach Notification Response Team - Privacy Breach Standard Operating Procedures, 3150.2.

1.2 Scope

This document provides the full SOP for the HUD Breach Notification Response Team (HBNRT) for handling and managing privacy related incidents, whether paper, electronic, or voice based. The standards established in this document are derived from various U.S. Laws, Federal Mandates, Presidential Directives, Federal Guidance, accepted industry standards, and best practices. This SOP includes in-depth information for assessing and responding to incidents and breaches involving Personally Identifiable Information (PII).

Section 4.0 of this SOP, pertaining to incident detection and reporting applies to all HUD employees, contractors, and third parties. A printable copy of Section 4.0 information for general HUD personnel can be found on the [HUD Privacy Website](#).



Once incidents and suspected incidents are reported to the HUD Help Desk, cybersecurity incidents will be escalated per Cyber Incident Response Plan (CIRP), which governs cybersecurity incident handling procedures.

1.3 Effective Date

This Handbook is effective as of 10/18/2021

2.0 Definitions

2.1 System of Records

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

2.2 Personally Identifiable Information

PII refers to information that can be used to distinguish or trace an individual's identity, individually or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII determination requires a case-by-case assessment of the specific risk that an individual can be identified, with recognition that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source—that, when combined with other available information, could be used to identify an individual.

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

2.3 Sensitive Personally Identifiable Information

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



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

2.4 Security vs. Privacy Incidents

A cybersecurity incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

A privacy incident, as defined by OMB Memorandum 17-12 is “An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security playbooks, or acceptable use policies.” Common examples of privacy incidents include using PII for purposes other than the stated purpose for which the information was originally collected, exceeding the retention period for PII, and collecting and/or using PII without first providing proper notice. The term “privacy incident” encompasses both suspected and confirmed incidents involving PII. Privacy incidents encompass PII maintained in electronic, paper, and voice-based format.

Not all cybersecurity incidents are privacy incidents and, conversely, not all privacy incidents are cybersecurity incidents, but some incidents can be both a privacy incident and a cybersecurity incident, as shown in the box in the center of Figure 3-1. If an incident involves both HUD IT Systems and PII, both the HUD Chief Information Security Officer (CISO) and HBNRT must collaborate to develop the appropriate reporting artifacts.

Privacy Incidents	Privacy & Cybersecurity Incidents	Cybersecurity Incidents
- Collecting/using PII without providing notice - Collecting PII without providing opportunity for consent for collection	- Network intrusions that gain unauthorized access to PII - Unauthorized use, storage, or disclosure of PII contained on HUD systems	- Denial of service attack - Malicious code - Unauthorized access to a system - Inappropriate system usage (e.g., threatening email)

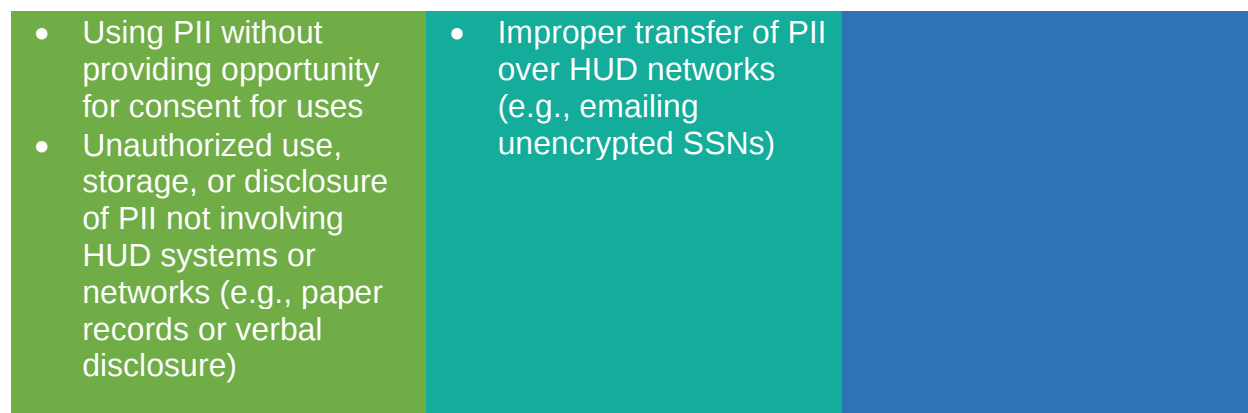


Figure 1: Cybersecurity vs. Privacy Incidents

2.5 Breach

Per OMB M-17-12, a breach is “the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized individuals and for any other than authorized purpose have access or potential access to PII in usable form, whether physical or electronic.”

2.6 Notice

Privacy safeguards that are required in the Privacy Act include permitting an individual to 1) determine what records pertaining to him or her are collected, maintained, used, or disseminated by agencies; 2) prevent records pertaining to an individual obtained by agencies for a particular purpose from being used or made available for another purpose without the individual's consent, and 3) gain access to information pertaining to himself or herself in agency records. The Privacy Act specifically requires notice via System of Record Notice (SORN) publication in the Federal Register whenever a SOR is established or revised (see Section (e)(4) of the Privacy Act). The Privacy Act also requires notice through its requirement for agencies to provide Privacy Act Statements to individuals whom the agencies are asking to supply information about themselves (see Section (e)(3) of the Privacy Act), when such information will be maintained in a SOR.

2.7 Harm

Harm means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII

maintained by the organization, including, but not limited to, administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

3.0 Privacy Incident Handling Roles and Responsibilities

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

3.1 HUD Breach Notification Response Team

The HBNRT is a core group of HUD privacy stakeholders who are responsible for managing a privacy incident lifecycle, including preparation, detection and risk analysis, triage and escalation, response and recovery, and coordination of any post-incident activities with the HUD SOC/CIRT.

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

3.2 General Responsibilities of Each Member

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

3.3 Specific Responsibilities of Each Member

3.3.1 Senior Agency Official for Privacy

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

3.3.2 Chief Privacy Officer

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



3.3.3 Chief Information Security Officer

- Work with the Chief Privacy Officer to ensure a complete and accurate privacy incident Report,
- Consult with the CIO, Deputy CIO, Associate CIO for Information Assurance, and Chief Privacy Officer concerning privacy incident handling,
- Work with the Chief Privacy Officer to contain privacy incidents,
- Work with the Chief Privacy Officer to assess the likely risk of harm posed by the privacy incident (e.g., low, moderate, or high impact) to determine who should handle the investigation, notification, and mitigation of the incident,
- Handle the investigation, notification, and mitigation for privacy incidents working with the Chief Privacy Officer,
- Collaborate with the Chief Privacy Officer to draft documents, as necessary, to support the privacy incident handling process,
- Make joint decisions with the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release in High and Moderate Impact privacy incidents that occurred and provide recommendations to the CIO,
- Make incident closure recommendations in consultation with the HBNRT, and
- Examine monthly reports issued by US-CERT addressing the privacy incidents that were reported to US-CERT.

3.3.4 Assistant Secretary for Congressional and Intergovernmental Relations

- Consult and coordinate with the CISO and Chief Privacy Officer to determine when notification of the Congressional Oversight Committee Chair is necessary for a privacy incident,
- Send notification to the Congressional Oversight Committee chair when an incident is deemed a “major incident,” and
- Respond to Congressional inquiries related to privacy incidents.

3.3.5 Associate Chief Information Officer for Information Assurance

- Advise the CIO and the Deputy CIO on all matters pertaining to privacy and the privacy/security interface, and



- Consult with the CIO, Deputy CIO, CISO, and Chief Privacy Officer concerning privacy incident handling.

3.3.6 Chief Financial Officer (CFO)

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

3.3.7 Chief Information Officer

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

3.3.8 Chief Procurement Officer

- Address credit monitoring acquisition requirements when it is determined

that credit monitoring will be offered.

3.3.9 Customer Relationship Manager

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

3.3.10 General Counsel

- Provide legal advice to the HBNRT regarding the potential for disciplinary action or corrective action against HUD personnel arising from a privacy incident,
- Provide recommendations to the CISO and Chief Privacy Officer in consultation with other members of the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release,
- Provide advice on whether referral of a privacy incident to other authorities is warranted,
- Serve as the Department's official legal representative in any formal administrative or judicial proceedings that might arise as a result of a suspected or actual breach, and
- Review, revise, and comment on reports and corrective actions taken.

3.3.11 General Deputy Assistant Secretary for Public Affairs

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

3.3.12 Human Capital Officer

- Work with the CFO, Chief Privacy Officer, or other members of the , as needed, in privacy incidents involving individuals' bank account numbers to be used for the direct deposit of credit-card reimbursements, government employee's salaries, or any benefit information,
- Consult with the Secretary or designee(s) in cases involving potential disciplinary or corrective action arising from a privacy incident, and
- Maintain a record of all disciplinary or corrective actions taken against HUD personnel that arise out of a privacy incident.

3.3.13 Inspector General

- Consult with the CISO and Chief Privacy Officer on a case-by-case basis to determine the appropriate incident handling procedures for Moderate and High Impact privacy incidents, as warranted,
- Provide recommendations to the CISO and Chief Privacy Officer, in consultation with other members of the HBNRT, regarding the propriety of external notification to affected third parties and the issuance of a press release, Conduct an investigation to determine:
 - o If the breach was intentional,
 - o If employee misconduct was involved,
 - o If the breach was a single incident or part of a broad-based criminal effort;
 - o If the incident is part of an ongoing investigation by the Federal Bureau of Investigation, Secret Service, or other federal, state, or local law enforcement, and,
 - o If notice to individuals or third parties would compromise an ongoing law enforcement investigation,
- Incidents involving potential employee involvement in incidents (i.e., employee misconduct) will be referred to the Office of the Inspector General (IG) Office of Special Investigations, which is authorized to conduct employee misconduct investigations, and
- Notify the Attorney General of any criminal violations relating to the disclosure or use of PII and Covered Information as required by the Inspector General Act of 1987, as amended.

3.3.14 Affected Program Manager

- Ensure compliance with federal laws and Departmental privacy policy concerning the operation and maintenance of information systems and programs,
- Recognize privacy incidents,
- Understand the privacy incident-reporting process and procedures
- Understand how to contact the HUD National Help Desk when a privacy incident occurs,
- Receive initial reports from HUD personnel regarding the possible detection of privacy incidents,
- Consult with the Chief Privacy Officer when necessary to obtain guidance

concerning privacy incident handling and other privacy issues affecting information systems,

- Assist the CISO and Chief Privacy Officer with the development of facts for the Privacy Incident Report, and
- Assist with the investigation and mitigation of a privacy incident to the extent necessary.

3.3.15 Affected Office Manager

- Ensure compliance with federal laws and Departmental privacy policy concerning the operation and maintenance of information systems and programs,
- Recognize privacy incidents,
- Understand how to contact the HUD National Help Desk when a privacy incident occurs,
- Receive initial reports from HUD personnel regarding the possible detection of privacy incidents and ensure all suspect and actual incidents within the office are reported to the HUD Help Desk,
- Inform the Program Manager of any suspected or actual incidents that are reported to the HUD Help Desk,
- Obtain guidance, when necessary, concerning privacy incident handling and other privacy issues affecting information systems,
- Assist the CISO and Chief Privacy Officer with the development of facts for the Privacy Incident Report, and
- Assist with the investigation and mitigation of a privacy incident to the extent necessary.

3.3.16 Senior Advisor to the Secretary

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

3.4 Other Individuals and Entities

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

3.4.1 Deputy Secretary

- Consult with HUD senior officials regarding the handling of privacy incidents

as warranted by the circumstances, and

- Provide recommendations to the Secretary, in consultation with members of the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release.

3.4.2 Chief Operating Officer

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

3.4.3 Deputy Chief Information Officer

- Act as Chair of the HBNRT in the SAOP's Senior Agency Official for Privacy's (SAOP) absence,
- Receive immediate notification of privacy incidents reported to the US-CERT, and
- Advise the CIO on the applicability of privacy incidents for communication to the White House.

3.4.4 HUD Computer Incident Response Team (HUD SOC/CIRT)

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

3.4.5 HUD Help Desk

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

3.4.6 HUD Personnel

- Attend periodic Privacy Awareness Training and Education,
- Maintain the privacy and security of all PII,



- Recognize privacy incidents,
- Upon the detection or discovery of suspected or confirmed incidents involving PII, contact the Program Manager or other “responsible official,” such as a supervisor,
- Use PII only for the purposes intended, and
- Follow all HUD procedures for the use, dissemination, and storage of PII.

3.4.7 Associate CIO for Service Delivery

- Notify the CISO and Chief Privacy Officer when a reported incident involves PII, and
- In the absence of the Chief Privacy Officer, notify HUD Security Operations Center/Cyber Incident Response Team (SOC/CIRT).

3.4.8 HUD Third Parties

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

4.0 Privacy Incident Response Process

4.1 Incident Detection and Reporting

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

4.1.1 Initial Discovery and Reporting Procedures

After confirming that the incident has been reported, **Office Managers** must inform the **Program Manager** of the incident for awareness.

1. Upon discovery of a suspected or verified privacy incident, **HUD personnel must immediately inform the HUD Help Desk.**
 - a. The **HUD Help Desk** can be reached at **1-888-297-8689 (Select Option 9 for assistance).**
2. After reporting the incident to the HUD Help Desk, **HUD personnel** must inform their **Office Manager** of the incident.