Senior Agency Official For Privacy

2020

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 2020 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

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			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			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			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		
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	Submitted to Agency	3	3	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CFO	Submitted to Agency	5	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CPD	Submitted to Agency	3	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CPO	Submitted to Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ODOC	Submitted to Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ENFC	Submitted to Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FHEO	Submitted to Agency	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GNMA	Submitted to Agency	0	6	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HSG	Submitted to Agency	18	7	25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OCIO	Submitted to Agency	2	12	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OGC	Submitted to Agency	2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OIG	Submitted to Agency	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDR	Submitted to Agency	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PIH	Submitted to Agency	5	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
REAC	Submitted to Agency	3	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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			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			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			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		
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
ODEEO	Submitted to Agency	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Agency Totals		43	31	74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

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.

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.			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	Submitted to Agency	3	0	**3**	2	0	**2**
CFO	Submitted to Agency	10	0	**10**	4	0	**4**
CPD	Submitted to Agency	7	3	**10**	2	2	**4**
CPO	Submitted to Agency	6	0	**6**	4	0	**4**
ODOC	Submitted to Agency	0	0	**0**	0	0	**0**
ENFC	Submitted to Agency	0	0	**0**	0	0	**0**
FHEO	Submitted to Agency	0	2	**2**	0	1	**1**
GNMA	Submitted to Agency	2	7	**9**	0	0	**0**
HSG	Submitted to Agency	60	30	**90**	12	2	**14**
OCIO	Submitted to Agency	19	41	**60**	3	5	**8**
OGC	Submitted to Agency	3	0	**3**	3	0	**3**
OIG	Submitted to Agency	0	2	**2**	0	0	**0**
PDR	Submitted to Agency	20	8	**28**	4	2	**6**
PIH	Submitted to Agency	15	6	**21**	4	1	**5**
REAC	Submitted to Agency	13	10	**23**	0	0	**0**
ODEEO	Submitted to Agency	0	1	**1**	0	0	**0**
Agency Totals		158	110	**268**	38	13	**51**

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.)

Section 3C: Information Technology Systems and Privacy Impact Assessments

- 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).

74

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.

74

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

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)

Section 4: Systems of Records

• Systems of records include only information about an individual that is relevant and necessary to accomplish a purpose required by statute or executive order.
• SORNs remain accurate, up-to-date, and appropriately scoped.
• SORNs are published in the Federal Register.
• SORNs include the information required by OMB Circular A-108.
• Significant changes to SORNs have been reported to OMB and Congress.
• Routine uses remain appropriate and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected.
• Each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary.
• The language of each contract that involves the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals, is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees.
• The agency's training practices are sufficient to allow agency personnel to understand the requirements of the Privacy Act, OMB guidance, the agency's implementing regulations and policies, and any job-specific requirements.

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.)

No

Section 6: Social Security Numbers

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.)

N/A

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

No

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.)

N/A

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.)

N/A

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 has already eliminated all unnecessary collection, maintenance, and use of SSNs by the agency.)

N/A

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

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

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

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.)

No

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

No

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.)

N/A

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?

No

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?

No

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 exist; however, they are not fully documented and/or do not cover all relevant aspects

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?

No

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.)

N/A

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

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?

No

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 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.)

N/A

13b. Has the agency designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls?

No

13c. Has the agency developed and maintained a written privacy continuous monitoring strategy?

No

13d. Has the agency established and maintained an agency-wide privacy continuous monitoring program?

No

Section 14: Privacy Program Website

14a. Does the agency have a Privacy Program Page located at (or redirected from) 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.)

No

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

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.)

No

Section 14: Privacy Program Website

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.)

N/A

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?

No

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

U.S. Department of Housing and Urban Development

PRIVACY PROGRAM PLAN

MARCH 2020

Table of Contents

1. Introduction

The purpose of the HUD (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.

2. 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. 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. 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. 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. 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 an information system or the portion of a hybrid control that is implemented for an 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. 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. 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.

9. 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 (HVU). 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.

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]

9.1. 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 (HVU)

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 HVU 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. 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. 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.

John G. Bravacos
Senior Agency Official for Privacy
March 2020

U.S. Department of Housing and Urban Development

PRIVACY PROGRAM PLAN

MARCH 2020

Table of Contents

1. Introduction

The purpose of the HUD (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.

2. 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. 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. 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. 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. 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 an information system or the portion of a hybrid control that is implemented for an 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. 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. 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.

9. 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 (HVU). 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.

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]

9.1. 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 (HVU)

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 HVU 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. 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. 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.

John G. Bravacos
Senior Agency Official for Privacy
March 2020

U.S. Department of Housing and Urban Development

PRIVACY INCIDENT RESPONSE PLAN

AUGUST 2020

Issue	Date	Pages Affected	Description
Version 1.0	**August 2020**	**All**	**Establishes HUD's Privacy Incident Response Plan for all HUD personnel.**

Table of Contents

Introduction

The HUD Privacy Incident Response Plan (PIRP) defines a framework for processes, communication, and roles and responsibilities for privacy incidents involving HUDs information and information systems. The PIRP ensures the proper procedures are in place to detect, analyze, respond, and recover from an actual, potential, or suspected privacy incident involving HUD's information and information systems.

The objective of the PIRP is to protect HUD's data, minimize loss or theft of information, and prevent disruption of critical services when incidents occur.

To accomplish this objective, it is necessary to:

- Coordinate proactive activities to reduce the risk of privacy compromise, including abiding by HUD Privacy policies and best practices;
- Be aware of each individual's role and responsibilities in the incident reporting process;
- Understand and adhere by incident response procedures and ensure necessary parties are notified in a timely manner.

While the Cyber Incident Response Plan (CIRP) provides an approach for handling cyber-specific threats, the PIRP applies to *all* privacy related threats, both cyber and non-cyber. Although most incidents involve information technology, a privacy incident may also involve verbal exchange, paper handling, and or physical security.

Scope

The HUD PIRP applies to all HUD personnel (including contractors) with access to HUD information and information systems in any format.

Authorities

Federal Statutes

- Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]
- Title 6, U.S.C., Section 142, "Privacy Officer"
- Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]

OMB Regulations and Guidelines

- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources (updated July 28, 2016)
- OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
- OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

Definitions

Privacy Incident

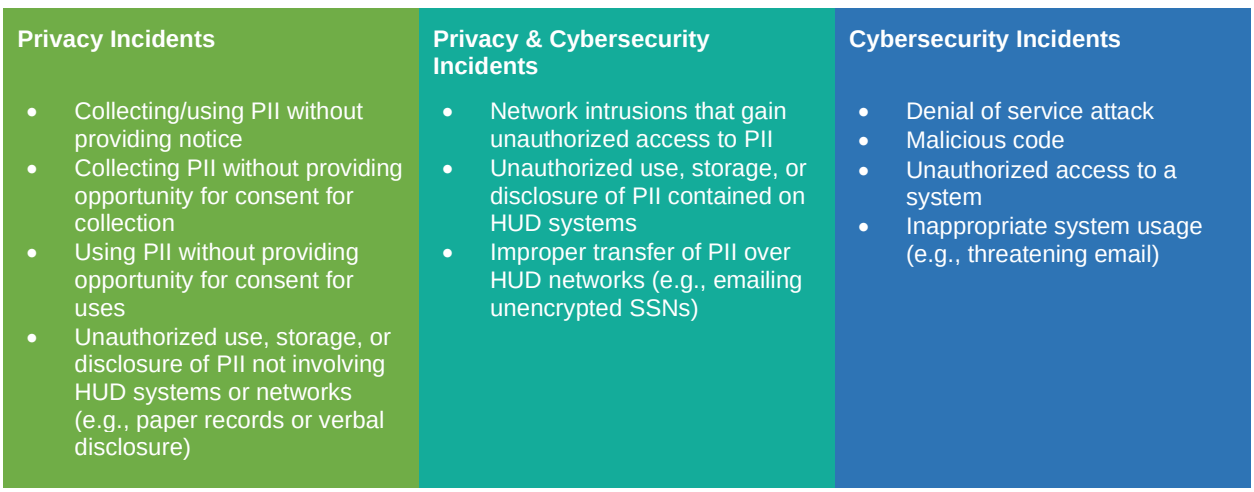
A privacy incident as defined by OMB Memorandum 17-12 is "An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security playbooks, or acceptable use policies."

There are many types of privacy incidents, including but not limited to using PII for purposes other than the stated purpose for which the information was originally collected, exceeding the retention period for PII, and collecting and/or using PII without first providing proper notice. The term privacy incident encompasses *both suspected and confirmed incidents* involving PII and applies to information in *both electronic and paper format*.

Cybersecurity Incident

A cybersecurity incident as defined by NIST Special Publication (SP) 800-53 Revision 4 is "any occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or, constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." Not all security incidents are privacy incidents and, conversely, not all privacy incidents are security incidents, but some incidents can be both a privacy incident and a security incident, as shown in the box in the center of Figure 1. Note that while this is intended to be a representative sample, this is not intended to be an exhaustive list.

Figure 1: Cybersecurity vs. Privacy Incidents



Personally Identifiable Information (PII)

For the purposes of this guidance, PII is defined as information which can be used to distinguish or trace a data subject's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Some examples include full names, social security numbers, telephone numbers, credit card numbers, driver's license numbers and biometric identifiers. Please refer to the HUD Privacy Policy for details regarding examples of PII and general guidance on proper PII handling.

Privacy Incident Response Procedures

Initial Discovery and Reporting

Once discovered, **HUD personnel** should report all privacy and cybersecurity incidents that are either suspected and/or confirmed to their **Office manager**.

- If you are unsure if something is an incident, report it to your **Office manager** and ask for assistance.
- If you are unable to reach your **Office manager**, call the **HUD Help Desk** at 1-888-297-8689 (Select Option 9 for assistance).

Office managers should coordinate with their **Privacy Liaison Officers (PLOs)**, **Security Operations Center (SOC)**, and the **HUD Help Desk** to determine if the incident is a privacy incident, cyber incident, or both.

- Contact the **HUD Help Desk** at 1-888-297-8689 (Select Option 9 for assistance).
- Contact **SOC** at cirt@hud.gov

Responding to Privacy Incidents

All incidents that are determined to be privacy incidents (cyber and non-cyber) should be reported to the Privacy Office. Office managers should complete and submit the HUD Privacy Incident Report as explained below *within one hour of discovering the incident.*

The HUD Privacy Incident Report should be sent to the Privacy Office at privacy@hud.gov.

HUD Privacy Incident Report

The PLOs for the Office where the incident occurred should fill out the HUD Privacy Incident Report Template. The report should include basic facts regarding when the incident occurred, when the incident was discovered, information about the nature of the incident, and whether the suspected incident involves PII. If the incident was also a cybersecurity incident, include the HUD system identifiers for all systems involved in the incident.

The PLOs for each Office are responsible for overseeing the documentation process and coordinating with Office managers and personnel to ensure all necessary information is collected and reported to the Privacy Office. While not all information may be available at the outset, the affected Office should gather as much information as possible for submission to the Privacy Office *within one hour of discovery.*

Responding to Cyber Privacy Incidents

In addition to the HUD Privacy Incident Report, if the privacy incident is also a cybersecurity incident, please refer to the HUD (CIRP) and coordinate with **SOC** for further steps.

- Contact **SOC** at cirt@hud.gov

Privacy Incident Roles and Responsibilities

HUD Breach Notification Response Team (HBNRT)

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

In collaboration with the Privacy Office, 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. The HUD Breach Notification Policy and Response Plan (HBNRP) outlines HUD's full approach for coordinating a response to a privacy incident.

General Personnel

- All **HUD personnel** should report actual and suspected privacy and cybersecurity incidents to their **Office manager**.
- After initial reporting, **HUD personnel** should also coordinate with **Office managers**, **PLOs**, and **SOC** as necessary to respond to incidents and breaches.

Office Managers

- **Office managers** are responsible for coordinating with **PLOs**, the **HUD Help Desk**, and **SOC** to determine whether an incident is a privacy incident, cybersecurity incident, or both.
- After initial reporting, **Office managers** should also coordinate with **PLOs**, the **Privacy Office**, **SOC**, and the **HBNRT** as necessary to respond to incidents.

PLOs

- **PLOs** should coordinate with **Office managers**, the **HUD Help Desk**, **SOC**, and the **Privacy Office** to assess what kind of incident occurred and how to properly report and document the incident.
- **PLOs** are responsible for ensuring incidents that occur within their Offices are properly reported to the **Privacy Office** via the HUD Privacy Incident Report template.

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-0001

OFFICE OF ADMINISTRATION

MEMORANDUM

RE: **Continuous Monitoring Strategy**
FROM: **Amy Morath, Acting Director, Office of the Executive Secretariat**
John Bravacos, Senior Agency Official for Privacy
DATE: **October 4, 2018**

According to OMB Circular A-130, each agency is required to develop and maintain a privacy continuous monitoring strategy. A privacy continuous monitoring strategy is a formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

At the time of this memorandum, the Department of Housing and Urban Development does not have a final privacy continuous monitoring strategy document. This guidance is in development and has not been reviewed by the appropriate officials and HUD senior leadership. The Department will continue to work on this formal document and develop a formalized policy.

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

U.S. Department of Housing and Urban Development

Guide to Develop Plans of Action for Minimizing Personally Identifiable Information

July 29, 2010

Table of Contents

List of Tables

1 Introduction

In May 2007, the Office of Management and Budget (OMB) issued memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable that called for the elimination of all unnecessary collection and use of personally identifiable information (PII), especially the Social Security Number (SSN) because of its sensitivity and high risk to privacy. In response, the U.S. Department Housing and Urban Development submitted a memorandum entitled, *Use of Social Security Numbers and other Personally Identifiable Information at the Department of Housing and Urban Development*. The memorandum documents HUD's commitment to eliminating the unnecessary collection and use of all personally identifiable information (PII), including the SSN.

A robust sampling of the HUD forms and Privacy Impact Assessments available on the HUD public website reveals a substantial collection of PII that should be assessed to determine whether its collection is authorized and necessary:

- PII
  - Approximately 80 percent of HUD forms sampled collect some type of PII.
  - Approximately 50 percent of systems listed collect some type of PII.
- SSN
  - Approximately 10 percent of HUD forms sampled ask for SSNs, and an additional 10 percent of the forms have TINs, which can function similarly to an SSN.
  - Approximately 43 percent of systems listed (including those listed as not having PII) had SSNs, and approximately 86percent of the systems that had PII also had SSNs.

The *U.S. Department of Housing and Urban Development Guide to Develop Plans of Action for Minimizing Personally Identifiable Information* (Guide) provides a framework for developing Plans of Action (POA) to implement PII, including SSNs[1], minimization. Section 5 of the Guide outlines HUD policies for minimizing collection and use of PII and SSNs. Section 6 provides a standard operating procedure (SOP) for developing POAs for specific collections of PII or SSNs. Section 7 delineates the steps for sustaining a minimized use of PII and SSNs in the future.

2 Purpose

The Guide outlines HUD policy for minimizing PII and helps HUD Program Managers effectively eliminate unnecessary collection and use of SSNs and to minimize PII, as appropriate. The scope of this effort includes all PII and SSNs, including full and truncated SSNs; SSNs from the public, HUD Personnel, and HUD contractors; and other uses of SSNs, such as the Taxpayer Identification Number (TIN).

3 Authorities for Producing the Guide

- Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual Persons," 1943.

[1] While SSNs are included within the definition of PII, per the focus of OMB M-07-16, this document references both SSNs and PII to emphasize SSNs as a particular area of attention for reduction within the context of minimizing all PII collections.

- Executive Order 13478, "Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers," 2008.
- HUD Information Security Procedures 2400.25 REV-2, November 30, 2009.
- OMB Memorandum M-07-16, "Safeguarding Against and Responding to Breach of Personally Identifiable Information" May 22, 2007.
- OMB Memorandum M-10-15, "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," April 21, 2010.
- OMB Memorandum, "Identity Theft Data Breach Notification Guidance," September 20, 2006.
- OMB Memorandum, "Recommendations for Identity Theft Related Data Breach Notification Guidance" September 20, 2006.
- President's Identity Theft Task Force, "Recommendations for Combating Identity Theft," April 2007.
- U.S. Department of Housing and Urban Development Breach Notification Policy and Response Plan, Draft Version 3.0, 1 February 2010.
- U.S. Department of Housing and Urban Development Memorandum FY-08, "Use of Social Security Numbers and other Personally Identifiable Information at the Department of Housing and Urban Development."
- U.S. Department of Housing and Urban Development Privacy Impact Assessment Questionnaire.
- U.S. Department of Housing and Urban Development, System Development Methodology, Release 6.06, January 2009.

4 Definitions

4.1 Personally Identifiable Information

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

Some examples of PII include name, date of birth (DOB), email address, mailing address, medical history, 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]

4.2 Sensitive Personally Identifiable Information

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

[2] OMB Memorandum M-07-16, "Safeguarding Against and Responding to Breach of Personally Identifiable Information" May 22, 2007

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

5 Roles and Responsibilities

5.1 Program Manager

- Completes the Initial Privacy Assessment (IPA).
- Complete the PII/SSN Minimization Checklist.
- Develops a POA to minimization HUD collection of PII.
- Collaborates with the Privacy Officer to revise POAs as necessary.
- Implements the POA in collaboration with relevant HUD offices.
- Reports status of all POAs to the Privacy Officer monthly, at minimum.
- Collaborates with IT Operations and Privacy Office to determine best means for the retention or destruction of PII data.

5.2 Privacy Officer

- Manages the PII Minimization Process.
- Reviews all IPAs and PII/SSN Minimization Checklists.
- Provides guidance to Program Manager regarding acceptable mitigation strategies in collaboration with HUD CIO and the HUD Chief Information Security Officer (CISO).
- Designates a staff member to participate as a member in the Review Team (also includes IT Operations, Office of Information Security, Office of System Integration and Efficiency, and Enterprise Architecture) to review the POA for appropriateness.
- Reports status of all POAs to the HUD CIO monthly.
- Establishes connections with HUD departments currently engaged in oversight and review of changes to systems, forms, and business processes.
- Collaborates with the appropriate organization within the HUD Office of the CIO to include PII and SSN specific checkpoints within the HUD System Development Methodology (SDM).
- Establishes ongoing information exchange relationships with the IT departments integrated with the data processing and risk assessment functions in the SDM process.
- Enhances the PIA process to ensure that only acceptable PII collections and uses occur, including the collections and uses of the SSN.
- Maintains and annually verifies HUD inventory of all PII collection.
- Conducts an awareness campaign to support PII minimization efforts.

5.3 Chief Information Officer (CIO)

- Provides guidance to Program Manager regarding acceptable mitigation strategies in collaboration with Privacy Officer and the HUD CISO.
- Makes budget decisions relevant to POAs.
- Approves alternative timelines for implementing POAs.

5.4 Senior Agency Official for Privacy (SAOP)

- Reviews and decides whether to accept appeals from Program Managers regarding the determination of authority to collect PII.
- Approves the elimination of the SSN within a particular system or form.

5.5 Forms Management Officer

- Supports the review of HUD forms for PII minimization.
- Supports the revision/creation of HUD forms to minimize the collection of PII in accordance with approved POAs.
- Reports on the status of all forms collecting PII to the HUD CIO annually.

5.6 Enterprise Architecture Representative

- Participates as a member in the Review Team (also includes the Privacy Office, IT Operations, Office of Information Security, and Office of System Integration and Efficiency) to review the POA for appropriateness.
- Reports status of all systems collecting PII, including SSNs, to the HUD CIO annually.

5.7 Chief Information Security Officer (CISO)

- Provides guidance to Program Manager regarding acceptable mitigation strategies in collaboration with Privacy Officer and the HUD CIO.
- Designates a staff member to participate as a member in the Review Team (also includes Privacy Office, IT Operations, Office of System Integration and Efficiency, and Enterprise Architecture) to review the POA for appropriateness.

5.8 IT Operations Representative

- Participates as a member in the Review Team (also includes the Privacy Office, Office of Information Security, Office of System Integration and Efficiency, and Enterprise Architecture) to review the POA for appropriateness.

5.9 Office of System Integration and Efficiency Representative

- Participates as a member in the Review Team (also includes the Privacy Office, IT Operations, Office of Information Security, and Enterprise Architecture) to review the POA for appropriateness.

6 HUD Policy for Minimization Plans of Action for Social Security Numbers and Personally Identifiable Information

6.1 PII Minimization Priorities

The first priority at HUD is eliminating the collection of unauthorized or unnecessary PII, particularly the SSN. Of any unauthorized or unnecessary collections, HUD will focus on system changes as key touch points because many form collections of PII are also entered into systems. PII elimination will be implemented through POAs that may also be prioritized. The HUD Chief Information Officer (CIO) and Privacy Officer will consider the following when refining the priorities of efforts:

- Enterprise impact of forms/systems collections
- Time to develop and release system change
- Level of potential risk of misuse associated with the PII or SSN
- Level of public scrutiny
- Level of oversight review
- HUD program priorities
- Cost estimates

Even as HUD develops strategic or high investment POAs to address unauthorized or unnecessary collections, all no/low cost options will be explored to ensure that the SSN elimination and PII reduction effort is timely. The HUD CIO makes all POA budget decisions.

The second HUD priority is to minimize risk to the PII that is necessary and authorized. Privacy risk mitigation will be implemented, focusing on appropriate PII handling, security procedures for access to systems, and security procedures for access to hardcopy materials.

6.2 Citations that Authorize HUD Collection of PII/SSNs

Policies and SOPs are not sufficient to demonstrate the authorization to collect PII or SSNs. For PII or SSNs to be collected a statute or executive order must provide authority for the collection and the collection must be appropriate.

Citations that authorize HUD collection of PII, or specifically SSNs, may include, but are not limited to :

- Computer Matching and Privacy Protection Act of 1988, Public Law 100-503, as amended
- Budget and Accounting Procedures Acts of 1921 and 1950, as amended
- Debt Collection Act of 1982, as amended
- Debt Collection Improvement Act of 1996, as amended
- Deficit Reduction Act of 1984, as amended
- Department of Housing and Urban Development Act
- Executive Order 10450, Security Requirements for Government Employment
- Executive Order 10577, Amending the Civil Service Rules and authorizing a new appointment system for the competitive service
- Executive Order 12353, Charitable Fundraising
- National Housing Act

- Government Employees Training Act of 1958 (U.S.C. Title 5, sections 4101 to 4118) Housing and Community Development Act of 1987
- Housing and Urban Development Act of 1965
- Internal Revenue Service, §6050 P(a) of U.S. Tax Code
- Office of Management and Budget (OMB) Circular A-129, "Managing Federal Credit Programs"
- Office of Management and Budget (OMB) Circular A-70, "Policies and Guidelines for Federal Credit Programs"
- Title 5, United States Code, Parts 731, 732, 736, 3301 and 3302, Civil Service and Personnel Investigations

6.3 Acceptable Uses of PII

6.3.1 Acceptable Uses of SSNs

Acceptable use of SSNs requires that the collection be authorized and necessary. HUD defines acceptable uses of SSNs as those that are provided for by law, require interoperability with organizations beyond HUD, or are required by operational necessities. Such operational necessities may be the result of the inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Those systems, processes, or forms that claim "operational necessity" shall be closely scrutinized. Ease of use or unwillingness to change is not an acceptable justification for this case.

The use of the SSN shall be limited to transactions that specifically require the presentation of the SSN to meet a statutory or regulatory requirement. Most applications that require the SSN for specific transactions do not require its use for every transaction. For example, systems that link to financial institutions may need the SSN for initial interactions, but thereafter use an account number or some other form of identification or authentication. As such, there is no need to use the SSN to authenticate individuals as part of every transaction.

Executive Order 13478 amended the Executive Order 9397 to rescind the blanket use of the SSN as a primary means of identification for individuals working for, with, or conducting business with the agency. The Office of Management and Budget will no longer accept the Executive Order 9397 citation as sufficient justification for the use of the SSN.

General categories of use that may continue to be acceptable for the SSN are listed in the table below. General coverage of an application by one of the following use cases must also take into account the particular way in which the SSN is used. The fact that a use case may loosely meet one or more of the justifications does not necessarily mean that a specific justification is acceptable. The Program Manager must examine specific legislative or regulatory language to determine if it is applicable. Justification for the use of the SSN in any one application does not constitute authority of use of the SSN in every transaction or interaction. Any transaction that includes transfer or presentation of the SSN should be scrutinized closely to determine if some alternate form of identification or authentication will suffice.

Table 1. Categories of Acceptable Use for the SSN

Authorized Uses	Description
HUD Authorities	HUD authorities for SSN collection are based in law, and their continued use must be mandated, not just authorized. Policies and SOPs are not sufficient to demonstrate the authority for collection or to justify continued use.
Law Enforcement, National Security,	Almost every law enforcement application must be able to report and track individuals through the use of the SSN. This includes, but is not limited to, checks of the National Crime

Authorized Uses	Description
Credentialing	Information Center; state criminal histories; and Federal Bureau of Investigation records checks.
Security Clearance Investigation or Verification	The initiation, conduct, or verification of security clearances requires the use of the SSN. The SSN is the single identifier that links all of the aspects of these investigations together. This use case is also linked to other Federal agencies whose use of the SSN as a primary identifier is both authorized and mandatory for their purposes.
Interactions with Financial Institutions	Federal law requires that individuals who hold accounts with financial institutions must provide the SSN as part of the process to open accounts. It may therefore be required for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions to provide the SSN.
Confirmation of Employment Eligibility	Federal statute requires that all persons employed within the United States must provide an SSN or comparable identifier to prove that he or she is eligible to work for or with the government of the United States. Any system that deals with employment eligibility must contain the SSN.
Administration of Federal Worker's Compensation	The Federal Worker's Compensation Program continues to track individuals through the use of the SSN. As such, systems, processes, or forms interacting with or providing information for the administration of this system or associated systems may be required to retain the SSN.
Federal Taxpayer Identification Number	The application of Federal and State income tax programs rely 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 must contain the SSN. Additionally, individuals who operate business vehicles may use their SSN as the tax number for that business function.
Data Matching with Other Agencies.	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 some other identifier as a primary means for transferring, matching, or checking information. These applications should be rigorously scrutinized to determine the availability of some other means of conducting these transactions.
Foreign Travel	HUD personnel may be required to travel beyond the borders of the United States, and many members often require official clearance prior to travel. Currently, the SSN is used as the identifier for these purposes.
Legacy System Interface	Many systems, processes, or forms that do not meet the criteria in the bullets above for the continued use of the SSN may not be able to transition to another identifier in a timely manner 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 plans are in place for the migration away from the SSN in the future. Plans to alter these use cases must take into account interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that the transfer away from the SSN does not cause unacceptably long interruptions to continued operations.
Other Cases	The previous categories may not include all uses of the SSN delineated by law. Should an application owner be able to show sufficient grounds that a use case not specified in bullets above is required by law, then that use case may continue to use the SSN. Any application that seeks to use this clause as justification must provide specific documentation in order to continue use under this justification.

6.3.2 Acceptable Uses of PII

Due to the nature of HUD's mission, PII is collected from employees, individuals applying for HUD programs, business partners, contractors, and clients. HUD shall collect only the PII elements necessary to support a HUD business process established by law. All other uses of PII are considered unacceptable.

Acceptable collection of PII requires that the collection of those specific elements be authorized and necessary. HUD defines acceptable collection of PII as those that are provided for by law, require interoperability with organizations beyond HUD, or are required by operational necessities. Such

operational necessities may be the result of the inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Those systems, processes, or forms that claim "operational necessity" shall be closely scrutinized to ensure that over collection of PII elements does not occur. Ease of use or unwillingness to change is not an acceptable justification for this case.

6.4 Acceptable Alternatives to the SSN

One of the primary reasons that many systems, processes, and forms shifted to use of the SSN is that it provided greater efficiency and required individuals to remember a single identifier. To counteract the vulnerability that this expanded use of the SSN created, HUD systems shall use alternatives to the SSN whenever possible. Truncation is not an adequate solution to the elimination/reduction of SSNs. If the Senior Agency Official for Privacy (SAOP) deems the use of SSNs unnecessary, the SSN must be eliminated regardless of truncation.

Alternatives include:

- **Electronic Data Interchange – Personal Identifier (EDI-PI).** The EDI-PI is a unique system identifier that is used for machine-to-machine transactions by HUD.
- **System-Specific Identifiers.** For use cases that are linked to a limited number of other applications, the best opportunity may be to create a unique identifier. In particular, for situations in which members of the public are required to gain access, particularly on a temporary basis, this may solve many privacy concerns. These identifiers can include alphabetic, numeric, and symbolic characters of varying lengths.
- **Net-Centric Environment.** A growing number of systems and processes are relying on authentication of individuals with a minimum of collection and storage of PII. These systems and processes rely on an authoritative data source for the storage of this PII, and access to that information is granted on an as-needed basis.
- **Elimination of Identifier.** HUD systems may be able to eliminate many instances where the SSN is collected or used. The technology associated with newer applications is such that it is possible to identify individuals specifically through other pieces of information, negating the need for a unique identifier. This situation is particularly true of applications that are finite in scope and do not interoperate with other applications.
- **Modification of Identifier.** Many processes in which HUD collects and uses an SSN can still function with a modified SSN. Modification includes masking the SSN upon entry into or display within the system so that the SSN is not visible to the user, combining the SSN in part with another form of identifier, etc.
- **Modification of Processes.** HUD may modify many instances where the SSN is collected or used to reduce the risk associated with the use of the SSN. HUD programs can mitigate the risk associated with authorized collections or uses of the SSN can be mitigated through training HUD personnel on the proper use and handling of electronic and paper SSNs, implementation of strict user roles to ensure that SSNs are only accessible to authorized individuals with a need to know, implementation of appropriate markings and handling instructions for print-outs, and implementation of chain of custody logs for extracts containing SSNs.

6.5 PII and SSN Risk Levels

Personally Identifiable Information under consideration for minimization includes PII that is not necessary for the business purpose for which it is collected, PII collected by HUD that is maintained in multiple instances, and PII that is maintained and disclosed through the use of extracts.

Social Security Numbers under consideration for minimization include full, truncated, and masked SSNs collected and maintained both on paper and in information technology (IT) systems. If a TIN or any other such number is issued to identify an individual in the same way that an SSN is used, it should be reported as an SSN and is subject to the SSN elimination and reduction initiatives.

Acceptable risk mitigation strategies must lower the associated level of PII or SSN risk. Variations of the PII and SSN are assigned different risk levels in order to 1) prioritize minimization efforts, e.g., HUD will focus on the high risk levels first, and 2) demonstrate risk mitigation efforts, i.e., high or medium risk SSNs may be modified to decrease the level of associated risk. At every risk level, HUD assumes that the collection and use of the PII and SSN are both authorized under law and mandatory.

The levels of PII and SSN risk are defined in the table below.

Table 2. PII and SSN Risk Levels

Risk Level	PII	SSN
High	• Authentication information, such as passwords • PII not necessary for the business purpose for which the PII is collected • PII maintained in extracts without an ongoing business justification • PII copied and maintained in multiple instances to support a single business process • Directly identifying PII in combination with other indirect identifying information, such as: – Race/ethnicity – Income/financial data (such as salary, federal taxes paid, bank account number, etc.) – Medical history/ information – Disability information – Criminal record	• Stand-alone SSNs visible to users in hard or electronic form • SSNs in combination with other direct identifying information, such as: – Name – Birth date – Birthplace – Home address – Home telephone – Personal email address – Mother's maiden name • SSNs in combination with other indirect identifying information, such as: – Race/ethnicity – Gender/ sex – Marital status – Spouse name – Number of children – Income/financial data (such as salary, federal taxes paid, bank account number, etc.) – Employment history – Education level – Medical history/ information – Disability information – Criminal record • SSNs in test and development environments
Moderate	• PII maintained in extracts for 90 days given an ongoing business justification • PII copied and maintained in multiple instances to support multiple business processes • Directly identifying PII in combination with other indirect identifying	• Truncated SSNs • Partially masked SSNs • Masked SSNs • Encrypted SSNs

Risk Level	PII	SSN
	information, such as: – Gender/ sex – Marital status – Spouse name – Number of children – Employment history – Education level	
Low	• PII maintained in extracts only for the duration necessary to support disclosure or transfer and then destroyed	• SSNs matched internally in the system but not visible to end-users

6.6 Privacy Risk Mitigation

PII, including SSNs, must be protected according to the level of sensitivity and risk to the individual's privacy, and controls to mitigate risk must be in compliances with the applicable laws, regulations, and guidance for information security. PII used for personal identity and authentication, including SSNs, are to be treated as having at least a moderate potential impact on an individual regarding the loss of confidentiality.[3] Any system deployed for a program involving this use of PII, including SSNs, must have security measures commensurate with this security categorization. This policy requirement shall apply whether the data resides on a system, transmits over a network, or is contained on physical digital or paper media.

After determining the PII Risk Level, the Program Manager, in coordination with the HUD Privacy Officer, CIO, and the CISO, will determine appropriate controls. Encryption, the application of which HUD encourages, will minimize the risk of unauthorized disclosure. Other security controls, such as password protection, may also mitigate the risk associated with unauthorized disclosure.

Additional actions to take to mitigate risk include, but are not limited to:

- Ensuring that hard copies with printed PII elements or SSNs include appropriate marking and handling instructions
- Masking electronically entered PII or SSNs upon entry
- Masking PII or SSN information that is visible to HUD personnel in either electronic or hardcopy form
- Truncation of SSNs[4]
- Limiting user roles with access to the PII or SSNs
- Managing extracts in accordance with OMB M-06-16
- Implementing chain of custody logs for extracts
- Additional training for personnel required to handle PII or SSNs

[3] National Institute of Standards and Technology (NIST) Special Publications (SP) 800-60 Volume 2, *Personal Identity and Authentication Information Security Category*, categorizes this as "confidentiality, Moderate."

[4] Truncation reduces the risk that the SSN may be used to cause financial harm through identity theft and, therefore, reduces the level of privacy risk associated with the use of an SSN. Truncated SSNs, how ever, are still considered SSNs and are not considered an appropriate substitute for SSNs that should be eliminated.

If the Privacy Officer deems the use of SSNs unnecessary, the SSN must be eliminated regardless of truncation.

6.7 Acceptable Timeframes

Minimizing the collection and use of the PII or SSNs requires significant time and resource investment, including the coordination of the Privacy Office with Information Technology (IT) Operations, the Office of Information Security, the Office of Systems Integration and Efficiency, and Enterprise Architecture. The following are guidelines for establishing acceptable timeframes in which a collection and/or use of PII or SSNs can be minimized in the POA:

- Complete a form revision within six months of establishment of a POA.
- Complete changes to a simple system, internal to HUD, with limited external sharing within 12 months of establishment of a POA.
- Complete changes to complex systems internal to HUD within 18 months of establishment of a POA.
- Complete changes to complex systems, with extensive sharing external to HUD, within 18 months of establishment of a POA.
- Complete changes to a business process that involves multiple systems within 24 months of establishment of a POA.

For POAs that do not fit the descriptions above, Program Managers will use the timeframes as guidance for proposing an acceptable timeframe. The Privacy Officer will review proposed timeframes and timeframes that exceed those listed above; timeframes will subsequently be subject to approval by the HUD CIO.

The Privacy Officer will collaborate with the Program Manager to establish a schedule for implementing the POA. Once the Privacy Officer and the Program Manager agree on the POA schedule, the Program Manager is responsible for tracking and reporting progress to the Privacy Officer.

6.8 Plan of Action Reporting

In order to ensure timely completion of POAs, the Privacy Officer will implement project management reporting for all POAs using the *Plan of Action Template* (contained within Appendix C).

POA reporting will use the following three-color code:

- **Red**. The date recorded in the POA has not been met; a revised date is necessary.
- **Yellow**. It is unlikely that the date recorded in the POA will be met.
- **Green**. It is likely that the date recorded in the POA will be met.

POA status cannot move from Green to Red; Program Managers must report Yellow status as soon as a schedule concern arises.

The Program Manager is responsible for tracking and reporting progress to the Privacy Officer. Program Managers shall use the POA to report on the status of PII and SSN minimization efforts to the Privacy Officer at least monthly and always prior to a schedule slip. The Privacy Officer shall report the status of all POAs by HUD Program to the HUD CIO at least monthly and always upon receiving notice from the Program Manager of a schedule slip.

6.9 Reporting Metrics

HUD shall report on metrics to demonstrate to HUD senior management the progress of PII minimization and SSN reduction efforts within on-going federal reporting efforts. These reports will also be used in concert with other Privacy Office reports (e.g., regarding Privacy Impact Assessments [PIA], System of Records Notices [SORN], incidents, etc.) to provide an overall assessment of agency Privacy compliance.

The HUD Privacy Officer will report monthly, or as requested, to the HUD CIO on the following:

- Status of Active POAs
- Number of Completed POAs
- Number of POAs accepted
- Number of POAs canceled as a result of Management Acceptance of PII Use
- Number of POAs outstanding

The HUD Forms Management Officer will report annually at a minimum, or as requested, to the HUD CIO on the following:

- Number of forms reviewed
- Number of forms requesting PII, "PII forms"
- Number of PII forms requesting SSNs
- Number of SSN justifications accepted and rejected
- Number of PII justifications accepted and rejected
- Examples of forms where SSNs were not allowed
- Examples of forms where PII data element collections were not allowed
- Examples of SSN masking or truncation

The HUD Privacy team will report annually, or as requested, to the HUD CIO on:

- Total number of systems collecting PII, "PII systems"
- Total number of PII systems collecting the SSN
- Number of new systems collecting PII, "new PII systems"
- Number of new PII systems collecting the SSN
- Number of existing systems where PII data element collections were reduced or eliminated, "existing PII systems"
- Number of existing PII systems no longer collecting the SSN
- Number of systems containing duplicated PII for a single business process

7 SOP for Minimization Plans of Action for PII and SSNs

The PII and SSN Minimization SOP details the steps necessary in order to develop the final PII/SSN POA. The SOP includes the steps from identifying collections of PII or SSNs to reducing the collection and minimizing the use of SSNs and PII, as appropriate. The SOP is provided below and is illustrated in the *PII/SSN Minimization Flowchart* (Appendix B). To aid in the process, Program Managers can use the *PII/SSN Minimization Checklist for Program Managers* found within Appendix D as necessary throughout the PII and SSN minimization effort to confirm that they are performing key responsibilities associated with the PII and SSN minimization effort. System Developers can use

the *PII/SSN Minimization Checklist for System Developers* also within Appendix D as necessary throughout the PII and SSN minimization effort to confirm that they are performing key responsibilities associated with the PII and SSN minimization effort.

Table 3. Standard Operating Procedure for Minimization Plans

SSN Inventory Creation (15 days)	
1.	Program Manager identifies collections and uses of SSNs in *Initial Privacy Assessment* (contained within Appendix C) and submits the *Initial Privacy Assessment* to the Privacy Officer. Go to Authority Determination.
Authority Determination (15 days)	
2.	Privacy Officer evaluates the authorities for PII collection and use identified by the Program Manager and determines whether sufficient authority exists, particularly for the SSN. Privacy Officer uses the *Minimization Plan of Action Template* (contained within Appendix C) to initiate a POA for the PII or SSN collection and records their authority determination on the POA. The Privacy Officer sends the POA to the Program Manager. The Privacy Officer may request that the Program Manager provide more information as necessary to make the determination. These questions may regard: the use of PII or SSNs in hard copy (forms and reports), the number of system connections and the degree of information sharing, Privacy Impact Assessments, System of Records Notices, use of extracts and chain of custody logs, etc.
Authority Determination (15 days)	
3.	Program Manager receives Privacy Office evaluation and accepts or appeals the Privacy Officer's determination.
	If accepted, the Program Manager develops a POA for minimizing PII or SSN collections and uses based on business and system needs in accordance with the *PII/SSN Minimization Checklist* (contained within Appendix C). **Go to Establishment of POA.**
	If rejected, the Program Manager can appeal.
3A.	Program Manager documents the appeal in the *Initial Privacy Assessment* and submits the appeal to the SAOP. The appeal should provide any necessary cost-benefit analysis on the use or substitution of the SSN, if applicable.
3B.	SAOP reviews appeal and determines whether PII or SSN collection is authorized, and, in particular, whether SSN use is mandatory.
	If the SAOP accepts the appeal, the Program Manager can continue the PII or SSN collection and use. However, the Program Manager still develops a POA to minimize risk associated with the PII or SSNs in accordance with the *PII/SSN Minimization Checklist.*
	If the SAOP denies the appeal, the Program Manager develops a POA for minimizing PII or SSN collections and uses based on business and system needs in accordance with the *PII/SSN Minimization Checklist*.
Establishment of a POA (30 days)	
4.	Program Manager evaluates business needs, systems needs, and existing forms in accordance with the *PII/SSN Minimization Checklist* and selects appropriate actions to document in the POA. The Program Manager, in coordination with the HUD Privacy Officer, CIO, and the CISO, will determine appropriate controls. If the Privacy Officer deems the use of SSNs unnecessary, the SSN must be eliminated regardless of truncation.
	Program Manager submits the draft POA and the *PII/SSN Minimization Checklist* to the Privacy Officer for review.
5.	A team consisting of the Privacy Office, IT Operations, Office of Information Security, Office of System Integration and Efficiency, and Enterprise Architecture representatives ("Review Team") reviews the POA for appropriateness. The reviewers shall consider when the POA is appropriate not only for the system for which the POA is developed by the Program Manager but for all the systems that may be involved in a given business process. For example, three systems may require the SSN for reciprocal machine-to-machine transactions such that while the SSN may be necessary for each system separately, upon evaluation, the business process should eliminate the SSN, and all three systems should use a substitute

	identifier.
5A.	If the Review Team determines the POA is acceptable, the Privacy Officer documents the date of approval on the POA. Proposed alternative solutions will be communicated to external business partners such as Public Housing Authorities, Federal Housing Administration partners, and Social Security Administration, as necessary according to HUD normal communications processes.
5B.	If the Review Team determines the POA is unacceptable, the Privacy Officer collaborates with the Program Manager until an acceptable version of the POA is created, and then the Privacy Officer documents the date of approval on the POA. Proposed alternative solutions will be communicated to external business partners such as Public Housing Authorities, Federal Housing Administration partners, and Social Security Administration, as necessary according to HUD normal communication processes.
POA Reporting	
6.	Program Manager reports monthly or as requested, whichever is more frequent, on the status of the POAs to the Privacy Officer using the POA.
7.	HUD Privacy Officer will report monthly or as requested to the HUD CIO on the following: • Status of Active POAs • Number of Completed POAs • Number of POAs accepted • Number of POAs canceled as a result of Management Acceptance of SSN Use • Number of POAs outstanding The Privacy Officer will use the *PII/SSN Minimization By Program Reporting Template* (contained within Appendix E).
7A.	HUD Forms Management Officer will report annually or as requested to the HUD CIO on the following: • Number of forms reviewed • Number of PII forms • Number of PII forms requesting SSNs • Number of PII justifications accepted and rejected • Number of SSN justifications accepted and rejected • Examples of forms where SSNs were not allowed • Examples of forms where PII data element collections were not allowed • Examples of SSN masking or truncation The Forms Management Officer will use the *PII/SSN Collection in Forms Template* (contained within Appendix E).
7B.	HUD Privacy Office will report annually, or as requested, to the HUD CIO on the following: • Total number of PII systems • Total number of PII systems collecting the SSN • Number of new PII systems • Number of new PII systems collecting the SSN • Number of existing PII systems where PII data element collections were reduced or eliminated • Number of existing PII systems no longer collecting the SSN • Number of systems containing duplicated PII for a single business process The HUD Privacy Officer will use the *PII/SSN Collection in Systems Template* (contained within Appendix E).
8.	CIO oversees agency progress.

8 Sustaining PII and SSN Minimization

In concert with efforts to minimize existing uses of PII and SSNs, HUD will enhance existing processes to ensure that Department programs and systems do not collect unnecessary PII,

including SSNs, without equivalent review of authorities and business justification. To sustain the ongoing effectiveness of these process changes, the HUD Privacy Office will establish connections with agency organizations currently engaged in oversight and review of changes to systems, forms, and business processes. Additionally, an awareness campaign focused on both leadership awareness and general employee education should achieve stakeholder acceptance and understanding of the process changes regarding the appropriate and allowable uses of PII and SSNs, as well as acceptable alternatives.

8.1 Technical Systems

To ensure technical systems are not built or changed to begin unnecessary collections of PII or SSNs, the Privacy Officer will enhance the process that guides technical systems development to incorporate PII and SSN specific validation checkpoints.

The HUD Privacy Officer will work with the appropriate organization within the Office of the CIO to include PII and SSN specific checkpoints within the HUD System Development Methodology (SDM), Release 6.06. The SDM currently incorporates privacy requirement checkpoints throughout the systems lifecycle, thereby offering leverage points to include PII and SSN specific validation questions.

The HUD Privacy Officer will work with the owner of the SDM to identify the points to include PII and SSN specific questions or deliverables, such as the Initial Privacy Assessment or PII/SSN Minimization Checklist. Existing deliverables identified as viable candidates for inclusion of PII and SSN checkpoints include the System Decision Paper Template and the System Security and Privacy Plan. Sections 4.1.14, 5.11, and 6.11 in the System Decision Paper template addressing privacy topics, and the System Security and Privacy Plan Authorization Memorandum signed by the project leader, Operations Division Director, program area/sponsor representative, and program area/sponsor director, are all eligible to have PII and SSN validation questions included.

Additionally, the HUD Privacy Officer will establish ongoing information exchange relationships with the IT departments integrated with the data processing and risk assessment functions in the SDM process. In many cases, each systems project underway receives support from the staff of these departments, positioning these teams to guide program managers and systems developers most effectively regarding the restrictions on collection and use of PII and appropriate alternatives to SSN use. The IT departments include Enterprise Architecture, the Quality Assurance Group, the Enterprise Data Management Group, and IT Security.

8.2 Forms Review

Per the HUD Privacy Act Handbook, Section 6-4, the HUD Privacy Officer currently inspects all new forms and is included in the review of existing forms. As part of the enhanced process, the HUD Privacy Officer engages with the program officials who own a form. The program officials complete the *PII/SSN Minimization Checklist* (contained within Appendix C) for new forms or verify the answers for existing forms in order to ensure a consistent evaluation of all SSN collection and to evaluate the necessity of collecting each PII element on the form

8.3 Privacy Impact Assessments

The Privacy Officer will enhance the current process for producing PIAs, to ensure that only acceptable PII collections and uses occur, including the collections and uses of the SSN. For new systems, existing systems, and new information requests that involve PII, including SSNs, HUD program managers will draft and submit a PIA to the HUD Privacy Officer for review. If the PIA

indicates a collection or use of PII or SSNs, the program manager will also complete and submit a *PII/SSN Minimization Checklist* (contained within Appendix C) to the HUD Privacy Officer for review. If the PII or SSN collection is not authorized or necessary, the Program Manager should create an alternative identifier in accordance with the Checklist. As a result, HUD will review PIAs and identify potential PII and SSN use and collection from the PIA before programs incorporate the PII or SSN into business processes.

8.4 Maintaining an Ongoing PII Inventory

The HUD Privacy Office will maintain the initial inventory of PII collections, including SSN collections, and uses created through the PII and SSN Minimization effort going forward. As HUD approves new technical systems or forms for collection or use of PII or SSNs, the Privacy Officer will add those collections to the ongoing inventory and specify in the inventory which collections maintain the SSN. Additionally, as HUD retires systems or forms, the Privacy Officer will remove systems from the inventory list and will revise the relevant PIAs and SORNs to reflect changes to systems collecting or maintaining PII, particularly the SSN. The Privacy Officer will issue the inventory annually to all owners of systems or forms that collect PII, including SSNs, for confirmation that their information is current and accurate.

8.5 Awareness

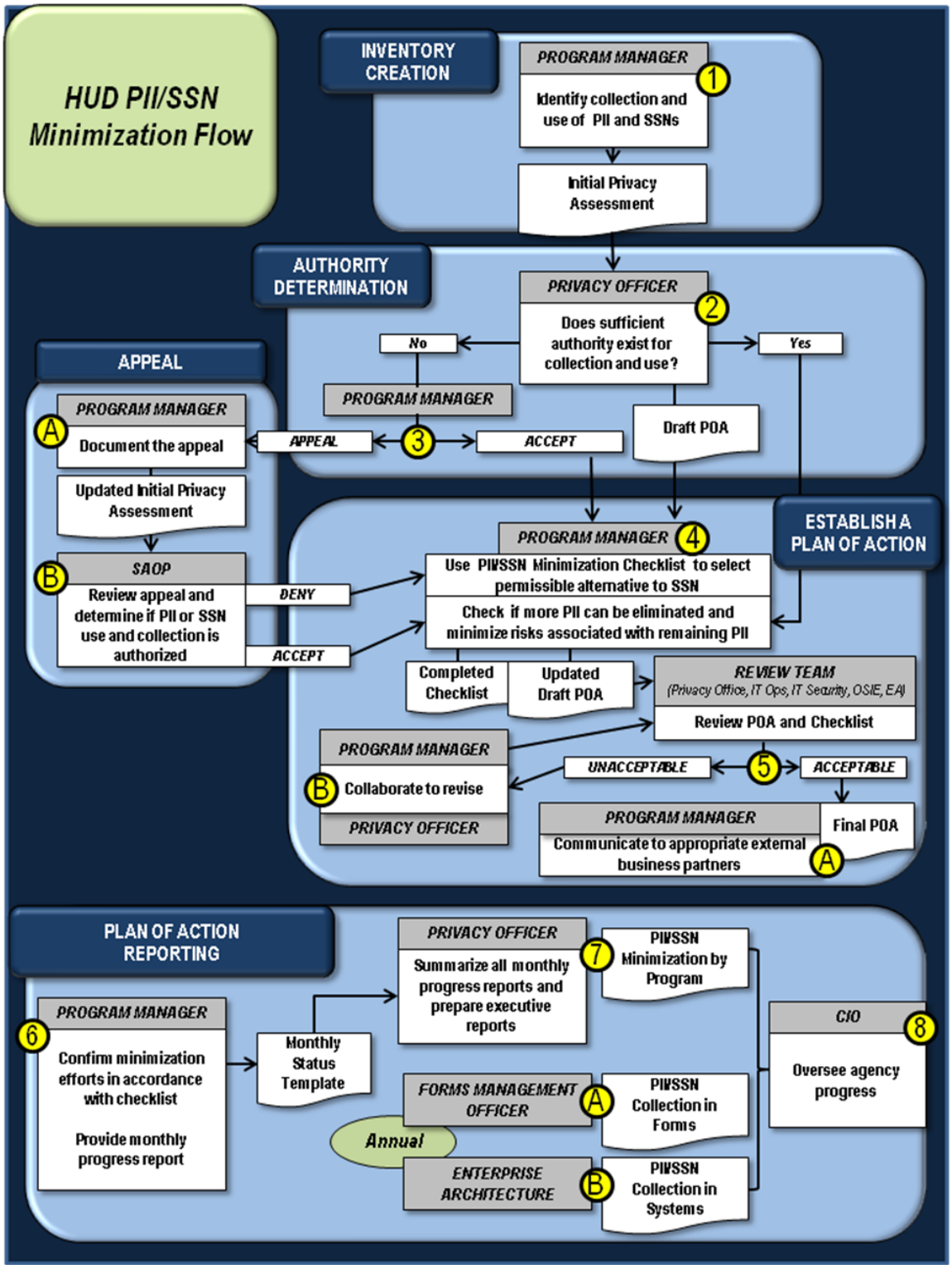
The HUD Privacy Officer will conduct an awareness campaign that focuses on informing all audiences of the above outlined process changes, as well as the updated policies and procedures for acceptable collections and uses of PII and SSNs and will include the following three distinct efforts:

- **Executive Communications.** The first effort will center on executive communications to key HUD leaders and their staffs. These briefings will outline the HUD definitions for acceptable uses, the policy for reducing the existing uses, the plans for ensuring new uses are not introduced unnecessarily, and the OMB reporting requirements.
- **Role-Based Education.** The second effort will focus on promoting education and awareness for personnel responsible for collecting and using PII or SSNs. This second effort will identify the primary roles within HUD related to PII or SSN collection and use and develop awareness materials targeted for that specific role. For example, system developers may receive training emphasizing the process changes to the SDM, and program managers may receive training emphasizing the Initial Privacy Assessment and PIAs.
- **Organizational Awareness.** Finally, the third effort will focus on increasing the awareness of the general HUD population through more general communication mechanisms, such as newsletter articles or weekly tips. The messages to this audience will focus not only on acceptable uses, but also on proper handling, retention and disposal, and a general point of contact (e.g., a generic privacy email box that is monitored by the staff of the HUD Privacy Office) where employees can submit questions.

Appendix A Acronyms and Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
DOB	Date of Birth
EDI-PI	Electronic Data Interchange – Personal Identifier
FHA	Federal Housing Administration
HUD	Housing and Urban Development
IPA	Initial Privacy Assessment
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PETs	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA	Plan of Action
SAOP	Senior Agency Official for Privacy
SDM	System Development Methodology
SOP	Standard Operating Procedures
SORN	System of Records Notice
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
TIN	Taxpayer Identification Number

Appendix B PII/SSN Minimization Flowchart



Appendix C Documents to Develop Plan of Action

C.1 Initial Privacy Assessment

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

INITIAL PRIVACY ASSESSMENT (IPA)

[Insert Name of Program Office]

Instruction & Template

[PROGRAM OFFICE]

[DATE]

INTRODUCTION

What is an Initial Privacy Assessment?

An Initial Privacy Assessment (IPA) is designed to assess whether a Privacy Impact Assessment (PIA), a Privacy Act system of records notice (SORN), and/or other related privacy documents are required. The responses to the IPA will provide a foundation for both a PIA and a SORN should either or both be required, and will also help to identify any policy concerns.

The IPA incorporates the matters previously addressed in the Department's Privacy Identifiable Information (PII) Survey, and thus replaces the survey.

When should an IPA be completed?

An IPA should be completed during the system's design phase, whether the system is electronic or contains only records in paper form, and should be completed before commencement of any testing or pilot project of an information system. Additionally, an IPA should be completed any time there is a change to the information system to determine whether there are any privacy issues as a result of such a change.

Who should complete the IPA?

The IPA should be written and reviewed by a combination of the component's (e.g., Privacy Act Officer, System Owner, Project Leaders), and the program-specific office responsible for the system.

How is the IPA related to the Capital Planning and Certification and Accreditation process?

Upon completion and approval of the IPA by the Privacy Officer the official document may be uploaded into the C&A tool, and provided as part of the IT Capital Planning process as validation of the completed evaluation. The completed IPA demonstrates that the program components have consciously considered privacy and related requirements as part of the overall system design. For an IT system that does not require a C&A, such as a minor application that runs on a system that does require a C&A, an IPA still should be completed to determine if other related privacy documentation are required for that system or project.

Where should the completed IPA be sent?

A copy of the completed IPA should be sent to the Office of Privacy via email to Donna.Robinson.Staton@HUD.gov and Nadine.Craft@HUD.gov. The Privacy Officer will review the IPA and determine what additional privacy documentation is required, and then will advise the Program component accordingly.

Initial Privacy Assessment

I. INFORMATION ABOUT THE PROJECT/SYSTEM

Date submitted for review:

Project Name/Acronym:

System Owner/Contact Information:

Project Leader/Contact Information:

1. Which of the following describes the type of records in the system:

☐ Paper-Only

☐ Combination of Paper and Electronic

☐ Electronic-Only

☐ **Other:** Please describe the type of project including paper based Privacy Act System of Records

*** Note:** For this form purpose, there is no distinction made between technologies/ systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.

2. Provide a general description of the system or project that describes: (a) the functionality of the system and the purpose that the records and/or system serve; (b) who has access to information in the system; (c) how information in the system is retrieved by the user; (d) how information is transmitted to and from the system; and (e) interconnections with other systems.

3. Have the IPA been reviewed and approved by the Departmental Privacy Officer

☐ YES

☐ NO (Please contact component privacy official before submitting official IPA.)

4. Status of System or Project

☐ This is a new system or project in development

Specify expected production date: **Do not complete Section II.**

☐ This is an existing system or project.

After completing Section I, complete Section II.

5. System or project personal identifiers/sensitive information

YES	NO	
☐	☐	**Does the system or project collect, maintain use or disseminate other personal identifiers/ sensitive information** (i.e., name, home address, home telephone number, date of birth, gender status, income/financial data. employment, medical history, criminal record, etc.)?

If yes, briefly describe the types of information about individuals in the system.

6. Does the information about individuals identify particular individuals (i.e., is the information linked or linkable to specific individuals, often referred to as personally identifiable information?)

☐ YES

☐ NO (If no, indicate below how the information is not identifiable to specific individuals.

7. Does the personally identifiable information in the system pertain only to government employees, contractors, or consultants?

☐ YES (If yes, specify individual type.) _____

☐ NO (If no, indicate below how the information is not identifiable to specific individuals.

8. Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover the system? (Please consult with the component's Privacy Act Officer if assistance is needed in responding to this question.)

☐ YES

☐ NO

9. SSN usage

YES	NO	Do the project or system collect, maintain, use, or disseminate Social Security Numbers (SSNs)? (This includes truncated SSNs)
☐	☐	

If yes, please provide the purpose/legal authority authorizing the solicitation of SSNs:

10. Is there a Certification & Accreditation record for your system?

☐ YES (If yes, indicate the following:)

Confidentiality	☐	**Low**	☐	**Moderate**	☐	**High**	☐	**Undefined**
Integrity	☐	**Low**	☐	**Moderate**	☐	**High**	☐	**Undefined**
Availability	☐	**Low**	☐	**Moderate**	☐	**High**	☐	**Undefined**

☐ NO (If no, please identify the FISMA-reported system whose C&A covers this system.)

☐ DO NOT KNOW

II. EXISTING SYSTEM OR PROJECT

1. When was the system developed?

2. If an existing system, has the system undergone any changes since April 17, 2003?

☐ YES (If yes, explain the nature of those changes and proceed to Question 3.)

☐ NO (If no, proceed to question 5.)

3. Do the changes to the system or project involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?

☐ YES

☐ NO

4. Please indicate if any of the following changes to the system or project have occurred: (Mark all boxes that apply.)

☐ A conversion from paper-based records to an electronic system.

☐ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

☐ A new use of an IT system, including application of a new technology that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and /or avenue for exposure of data that previously did not exist.)

☐ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

☐ A new method of authenticating the use of an access to information in the identifiable form by members of the public.

☐ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

☐ A new interagency use of shared agency function that results in new uses or exchanges of information in identifiable form.

☐ A change that results in a new use of disclosure of information in identifiable form.

☐ A change that results in new items of information in identifiable form being added into the system.

5. Does a PIA for the system already exist?

☐ YES (If yes, provide the date and title of the PIA and whether the PIA is posted on the Privacy Office webpage.

☐ NO.

IPA Determination/Approval

(To be completed by the Privacy Office)

DATE REVIEWED:
REVIEWERS NAME:

☐	**This is <u>NOT</u> a Privacy Sensitive Project – the project contains no personal identifiers/sensitive information**
☐	**This <u>IS</u> a Privacy Sensitive Project**
☐	PTA sufficient at this time
☐	A PIA is required
COMMENTS:	

_____ _____

Program Director Signature Date
[Title]

_____ _____

Departmental Privacy Officer Signature Date

C.2 PII/SSN Minimization Checklist

PII/SSN Minimization Checklist

The PII/SSN Minimization Checklist is a guide for Program Managers to identify PII minimization opportunities, especially related to the SSN. Use the checklist in conjunction with the Plan of Action to document and track status of PII/SSN Minimization efforts.

I. Assess SSN Use	**Yes**	**No**
1. Is the SSN shared as an identifier with other systems, (internal or external) to HUD?	☐	☐
a. If no, go to **Evaluate System SSN Needs.**	☐	☐
b. If yes, can both systems replace the use of the SSN?	☐	☐
i. If yes, go to **Evaluate System SSN Needs.**		
ii. If no, go to **Minimize Risk.**		
2. Can the process run without the SSN or similar identifier?	☐	☐
a. If yes, eliminate the data and form field. Go to **Confirm Minimization Efforts**.		
b. If no, go to **Evaluate System SSN Needs.**		
II. Assess PII Use	**Yes**	**No**
1. Is each PII data element identified?	☐	☐
a. If no, identify all PII data elements prior to proceeding.		
2. Is each PII data element necessary for the business purpose?	☐	☐
a. If yes, go to **Minimize Risk.**		
b. If no, identify unnecessary collections, document steps in POA to stop unnecessary collection, and assess feasibility of removing prior instances of data collection.		
3. Does the system have a Privacy Impact Assessment (PIA)?	☐	☐
a. If yes, revise the PIA to reflect the PII collected and used by the system, e.g., remove collection of the SSN and replace with the new identifier being collected, remove the collection of the PII, etc.		
b. If no, and the system is collecting, using, or modifying PII, conduct a PIA.		

II. Assess PII Use	Yes	No
4. Does the system have a System of Records Notice (SORN)?	☐	☐
a. If yes, revise the SORN to reflect what PII is collected and used.		
b. If no, and the system maintains PII and retrieves information by personal identifier, create a SORN to reflect what PII is collected and used.		
III. Evaluate System SSN Needs	**Yes**	**No**
5. Does the system require nine character spaces?	☐	☐
6. Does the system require numbers?	☐	☐
7. Can the system handle a combination of letters, numbers, and symbols?	☐	☐
8. Does the system require that the field be formatted in a certain way? (for example, xxx-xx-xxx)	☐	☐
9. Can the system be modified?	☐	☐
a. If yes, can an alternative identifier replace the SSN?	☐	☐
i. If yes, replace the SSN with the new identifier, which to the extent possible is alphanumeric, includes symbols, and is randomly generated.		
b. If no, then modify the SSN. Go to Minimize SSN Risk.		
10. Does the system have a Privacy Impact Assessment (PIA)?	☐	☐
a. If yes, revise the PIA to reflect the PII collected and used by the system, e.g., remove collection of the SSN and replace with the new identifier being collected.		
b. If no, and the system is collecting, using, or modifying PII, conduct a PIA.		
11. Does the system have a System of Records Notice (SORN)?	☐	☐
a. If yes, revise the SORN to reflect what PII is collected and used.		
b. If no, and the system maintains PII and retrieves information by personal identifier, create a SORN to reflect what PII is collected and used.		

IV. Minimize Risk	Yes	No
12. Is the PII or SSN printed in hard copy?	☐	☐
a. If yes, does the hard copy contain the appropriate marking and handling instructions?	☐	☐
i. If no, mark the hard copy and add the appropriate handling instructions. If unable, explain exception here:		
13. Is the PII or SSN entered electronically?	☐	☐
a. If yes, can the information be masked upon entry (e.g. SSN xxx-xx-xxxx)?	☐	☐
i. If yes, mask upon entry.		
ii. If no, provide training to HUD personnel on PII and SSN sensitivity and necessary protections.		
14. Is the PII or SSN visible electronically by HUD personnel?	☐	☐
a. If yes, can the information be masked?	☐	☐
i. If yes, mask the information to HUD personnel.		
ii. If no, provide training to HUD personnel on PII and SSN sensitivity and necessary protections.		
b. For SSNs that cannot be masked, can the SSN be truncated (e.g., xxx-xx-1234 or 1234)? Truncation is not an adequate solution to the elimination/reduction of SSNs. If the use of SSNs is deemed unnecessary, it must be eliminated regardless of truncation.	☐	☐
i. If yes, truncate the SSN.		
ii. If no, provide training to HUD personnel on SSN sensitivity and necessary protections.		
15. Are there user roles that limit those with access to the PII or SSN to authorized individuals with a need to know?	☐	☐
a. If yes, verify that users are authorized and have a need to know.		
b. If no, create users roles to ensure that only authorized individuals with a need to know have appropriate read/write access to the PII or SSN. If unable to create user roles, explain the exception here:		

IV. Minimize Risk	Yes	No
16. Is the PII or SSN contained in system extracts? See requirements for managing extracts outlined in OMB M-06-16.	☐	☐
a. If yes, are the extracts controlled through chain of custody logs?	☐	☐
i. If yes, are the extracts maintained within OMB guidelines?	☐	☐
1. If yes, confirm policies and procedures for destruction of extracts.		
2. If no, implement policies and procedures for destruction of extracts outside of OMB guidelines.		
ii. If yes, for extracts that are maintained for outside of OMB guidelines, has the Senior Agency Official for Privacy (SAOP) approved the retention of the extract for the additional time?	☐	☐
1. If yes, go to **Confirm Minimization Efforts**.		
2. If no, explain the exception here: Go to **Confirm Minimization Efforts**.		
b. If no, implement chain of custody logs for the extracts. If unable to implement chain of custody logs, explain the exception here:		
17. Are existing procedures sufficient to respond to potential breaches or incidents involving the SSNs at issue?	☐	☐
a. If no, propose necessary procedural updates to the Privacy Officer.		
V. Confirm Minimization Efforts	**Yes**	**No**
18. Is a form being used?	☐	☐
a. If yes, has the form been modified and approved by OMB?	☐	☐
i. If no, work with Records Management office to modify the form and secure OMB approval.		

V. Confirm Minimization Efforts	Yes	No
19. Have existing SSNs been replaced with new identifiers?	☐	☐
a. If no, work with IT Operations to schedule system change in an upcoming release according to priority timelines outlined in Section 6.7 of the *Guide to Develop Plans of Action for Minimizing PII* (the Guide).		
20. Are new records created using the new identifier?	☐	☐
a. If no, work with IT Operations and Program Manager to schedule system change in an upcoming release according to priority timelines outlined in Section 5.7 of the Guide, and address any program management concerns.		
21. Have unnecessary PII collections been stopped?	☐	☐
a. If no, work with IT Operations to schedule system change in an upcoming release according to priority timelines outlined in Section 6.7 of the Guide.		
22. Has the system changed?	☐	☐
a. If no, work with IT Operations to schedule system change in an upcoming release according to priority timelines outlined in Section 6.7 of the Guide.		
23. Record successful completion of PII/SSN Minimization according to the **Plan of Action**.		

Summary of Action Items (Select all that are applicable)	
Reduce PII Collection	☐
Substitute SSN	☐
Marking and Handling Instructions	☐
Mask	☐
Truncate	☐
Additional Training	☐
Restricted User Roles	☐
Manage Extracts	☐
Breach Management	☐
Form Revision	☐
Create/Revise PIA	☐

Create/Revise SORN	☐

C.2.1 Minimization Plan of Action

Minimization Plan of Action

PII Collection (specify in identifier whether collection includes SSN):

SSN Authority Determination: Authorized but not mandatory

PII Authority Determination: Authorized but not mandatory

Program Manager:

Replacement Identifier: EDI-PI

Program Office:

Status: Red

Date POA Approved:

Date POA Completed:

POA Schedule							
	Date Submitted	**Privacy Review**	**Privacy Approval**	**Date to be Implemented**	**Date Implemented**	**Status**	**Comments**
PII Reduction Plan							
Identify unnecessary PII							
Implement changes to stop collection							
SSN Replacement Plan							
Create replacement identifier							
Implement new identifier going forward							
Replace existing identifier previously created							
Form Revision							
Draft 1 New Form							
Draft 2 New Form							
Training							
Content Draft 1							
Content Draft 2							
Process Modification							
Proposed changes to SOP							
Approved SOP							

POA Schedule							
	Date Submitted	**Privacy Review**	**Privacy Approval**	**Date to be Implemented**	**Date Implemented**	**Status**	**Comments**
Program Management							
Marking and Handling Instructions							
Mask							
Truncate							
Restricted User Roles							
Manage Extracts							
Modify Breach Policy							
Create/Revise PIA							
Create/Revise SORN							

Appendix D PII/SSN Minimization Checklists

D.1 PII/SSN Minimization Checklist for Program Managers

Use the following checklist to analyze, strengthen, and develop needed SSN safeguards.

Guidance	Yes	No
I am active in helping employees that I manage/supervise to understand and determine when it is appropriate to collect and use Personally Identifiable Information (PII), including Social Security Numbers (SSN).	☐	☐
I keep a current list of employees that I manage/supervise who are authorized to collect/access PII/SSNs.	☐	☐
I ensure that PII/SSNs are stored on computers that are secured in compliance with current HUD IT Security Policies.	☐	☐
I am active in helping employees that I manage and/or supervise to understand and determine when and how to appropriately transmit or disclose PII/SSNs.	☐	☐
I keep a current list of employees that I manage and/or supervise who are authorized to release and provide PII/SSN data to government agencies and authorized third parties.	☐	☐
I keep a current list of government agencies and third parties who are authorized to receive PII/SSN data.	☐	☐
I ensure that government agencies and authorized third parties receiving PII/SSN, originating from the HUD, have appropriate policies, processes, and controls in place to safeguard the information.	☐	☐
I ensure employees that I manage and/or supervise are aware of PII/SSN safeguarding, processing, transmission, and disclosure responsibilities.	☐	☐
Prior to implementation of a new usage or process involving PII/SSN I engage the Privacy Impact Assessment (PIA) to review the privacy risks and identify potential requirements to the proposed process.	☐	☐
I ensure that employees I supervise and/or manage understand and follow HUD Record Management Policies and related Document Retention Schedules.	☐	☐
I ensure that employees I supervise and/or manage participate in training related to information safeguarding and PII/SSN data security.	☐	☐
I regularly track and monitor [xxx] reporting for employees I manage/supervise.	☐	☐

D.2 PII/SSN Minimization Checklist for Risk Mitigation

Use the following checklist to analyze, strengthen, and develop needed PII/SSN safeguards.

Guidance	Yes	No
I ensure that access controls are in place and adequate, in accordance with relevant HUD policies, to secure PII/SSN information.	☐	☐
I regularly review user access on systems that store PII/SSNs in accordance with current HUD access policies and IT Security rules.	☐	☐
I ensure that workstations and authorized portable devices, such as PDAs and laptops storing PII/SSNs, use strong encryption in accordance with current HUD standards and in accordance with IT Security rules.	☐	☐
I ensure that authorized employees transmitting or disclosing PII/SSNs to government agencies or authorized third parties have access to encryption technology to protect PII/SSNs being transmitted via email, file transfers, Web sessions, communication protocols, or other dedicated communications paths.	☐	☐
I ensure that PII/SSNs are only processed on technology systems that are appropriately secured and controlled according to IT Security policies.	☐	☐
I ensure that all applications and systems that process PII/SSNs meet access management, change management, and logging and monitoring standards and procedures.	☐	☐
I ensure that anti-virus software is configured to check all files, Internet downloads, and email.	☐	☐

Appendix E Reporting Templates

E.1 PII/SSN Minimization by Program-Reporting Template

Date:

Program by Program Status

Program Manager	SSN Collection	PII Collection	Replacement Identifier	Status
			EDI-PI	Red

Overall

Status of Active POAs	
POAs Accepted	
POAs Canceled	
Completed POAs	
POAs Needed	

E.2 PII/SSN Collection in Forms -- Summary Report

Annual Status of PII Collection in Forms

Date:

Overall

Status of Forms	Number/Description
Forms reviewed	
Forms requesting PII, "PII forms"	
PII justifications accepted and rejected	
Examples of forms where PII was not allowed	
PII Forms requesting SSNs	
SSN justifications accepted and rejected	
Examples of forms where SSNs were not allowed	
Examples of SSN masking or truncation	

E.3 PII/SSN Collection in Systems Summary Reporting

Annual Status of PII/SSN Collection in Systems

Date:

Overall

Status of Systems	Number	Status of Systems	Number
Systems collecting PII, "PII systems"		PII Systems collecting the SSN	
New Systems collecting PII, "new PII systems"		New PII systems collecting the SSN	
Existing systems where PII data element collections were reduced or eliminated, "existing PII systems"		Existing PII systems no longer collecting the SSN	
Instances of duplicated PII for a single business process			

Status	System Names
Systems collecting the SSN	
New PII systems collecting the SSN	
Existing PII systems no longer collecting the SSN	
PII Systems	
New PII Systems	

Status	System Names
Existing PII systems data element collections were reduced or eliminated	
Instances of duplicated PII for a single business process	

Appendix F Additional Best-practice Strategies for Sustaining Minimization

F.1 Enterprise Privacy Enhancing Technologies

HUD should consider augmenting PII minimization efforts with enterprise privacy-enhancing technologies (ePETs). The ePETs are data stewardship tools that help organizations manage sensitive information while achieving their business objectives. Although not always privacy specific, ePETs help organizations manage PII appropriately throughout the information lifecycle. ePETs functionality can enable context-sensitive access and use of data, prevent inappropriate access and use of data internally and disclosure of data externally, prevent data collected from being linked to an individual, facilitate transactions that reveal minimal PII, and automate privacy audit functions.

Commercially available ePETs include:

- **Data desensitization tools ("anonymization").** Desensitization tools mitigate the risk in static, structured datasets through a variety of manipulations, such as masking.
- **Content identification tools.** Content identification tools detect sensitive data at rest.
- **Policy enforcement tools.** Policy enforcement tools detect and act upon sensitive data in motion and in use. These tools are frequently offered as a suite of tools under the umbrella of "data loss prevention."
- **Structural compliance tools.** Structural compliance tools check the structure of Web pages and other constructs on an ongoing basis for compliance with privacy and other requirements.
- **Secure computation tools.** Secure computation tools detect common data across systems without revealing it.

Prior to implementation, HUD should establish a process for evaluating PETs produced by different vendors.

F.2 Sample SSN Minimization Plans from Government Agencies

- Department of Energy on the Use of the SSN, February 2009, http://management.energy.gov/documents/DOE_Guidance_on_the_Use_of_the_SSN.pdf
- Directive-Type Memorandum (DTM) 07-015-USD(P&R) – "DoD social Security Number (SSN) reduction Plan", March 28, 2008, http://www.dtic.mil/whs/directives/corres/pdf/pr080328ssn.pdf
- Eliminate Unnecessary Collection and Use of Social Security Numbers at the Department of Veterans Affairs, April 2008, http://www.privacy.va.gov/PRIVACY/docs/SSnApr2008FinE.pdf
- Eliminate Unnecessary Collection and Use of Social Security Numbers at the Department of Veterans Affairs, September 2007, http://www.privacy.va.gov/docs/SSNPlanFinal9-17-07.pdf
- Evaluating Holdings of Personally Identifiable Information (PII) and Eliminating Unnecessary Collections at the Department of Veterans Affairs, September 2007, http://www.privacy.va.gov/docs/PII_Plan_forFY2008_FISMA_RPT_Sept08.pdf