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