MEMORANDUM

September 13, 2018

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

To: Suzanne Israel Tufts
Assistant Secretary for Administration, A

From: Brian T. Pattison by
Assistant Inspector General for Evaluation, Office of Inspector General, G

Subject: HUD OIG Report: HUD Privacy Program, *2018-OE-0001*

We have completed our evaluation of the U.S. Housing and Urban Development (HUD) privacy program. This report highlights our findings and conclusions regarding this critical agency program. While a number of HUD privacy program aspects improved since we last evaluated the program in 2014, it continued to face challenges in establishing a program commensurate with the nature and volume of sensitive information held by the agency.

We observed increased prioritization and executive leadership support for the privacy program, and improved collaboration between the privacy and IT programs. HUD improved its privacy impact assessment processes and took a more active role to ensure privacy is properly addressed in the agency's technology and business operations. HUD also continued to improve its privacy awareness training provided to all employees. However, HUD had not established a strategic plan for privacy, and key initiatives were put on hold pending the staffing of key privacy program management positions. HUD had not integrated privacy risks into its enterprise risk management (ERM) process, had not formalized many compliance and oversight practices, and lacked a formal compliance program. Critically, HUD had still not been able to fully identify and inventory its extensive holdings of personally identifiable information (PII).

We have made 24 recommendations for improvements at both the operational and programmatic levels. We urge HUD to develop a corrective action plan for each recommendation and allocate the personnel and resources necessary to make the recommended improvements.

I greatly appreciate the professional assistance you and your staff provided throughout the evaluation. Please contact Director John Garceau at [redacted] or [redacted] if you have any questions.

Attachments

OIG Report: HUD Privacy Program Evaluation (2018-OE-0001)

Cc: Pamela Hughes Patenaude, Deputy Secretary
Pat Hoban-Moore, General Deputy Assistant Secretary for Administration
John Bravacos, Director, Executive Secretariat
David Chow, Chief Information Officer
Andrew Hughes, Chief of Staff
J. Paul Compton, Jr., General Counsel
Amy Thompson, Assistant Secretary for Public Affairs

This page intentionally left blank

OFFICE OF INSPECTOR GENERAL

OFFICE OF EVALUATION

U.S. DEPARTMENT
OF HOUSING
AND URBAN
DEVELOPMENT

HUD Privacy Program Evaluation Report

Information Technology Evaluations Division

Washington, DC Report Number: 2018-OE-0001 September 13, 2018

This page intentionally left blank

Office of Inspector General
Office of Evaluation
451 7th Street SW, Washington DC 20024
Phone (202) 708-0430, Fax (202) -401-2505
www.hudoig.gov

Executive Summary

HUD Privacy Program Evaluation Report

Why We Did This Evaluation

HUD is entrusted with the personal information of tens of millions of Americans. It is critical that HUD establish and resource a mature privacy program to meet its legal requirements and protect this sensitive information. A breach of this data would cause citizens undue difficulties and financial hardship. A breach may also create a lack of trust and unwillingness by external parties to share sensitive data with the agency, thereby jeopardizing HUD's ability to complete its mission.

Past OIG evaluations have identified resource deficiencies and other weaknesses within HUD's Privacy and IT programs.

We conducted this evaluation to determine the effectiveness of HUD's current privacy program. We assessed the adequacy of agency strategies, plans, controls and practices at the enterprise and program levels. We also examined the level of progress achieved since we last evaluated the program in 2014.

What We Recommend

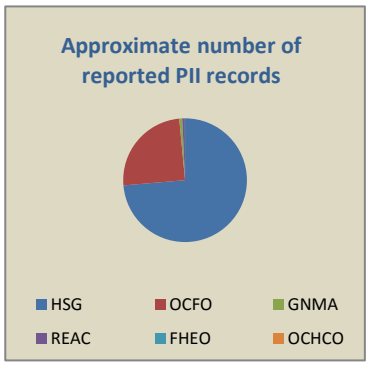
We recommend that HUD establish a strategic plan for its privacy program and fill key program positions within the privacy program with qualified personnel. We further recommend that HUD ensure adequate resources and privacy expertise; implement a formal compliance program; clarify privacy roles across the agency; develop the capability to identify and inventory all of its PII; and fully integrate the privacy program with other enterprise programs.

We urge HUD to address the 14 remaining open recommendations from our 2014 privacy program evaluation, and address the 24 additional recommendations listed in Appendix A of this report.

Results of Evaluation

The U.S. Department of Housing and Urban Development (HUD) maintains over one billion records containing personally identifiable information (PII) of American citizens. Figure 1 identifies the approximate number of PII records by major HUD program office.

Figure 1. PII records by Program Office



Program Office		Approximate number of PII records
HSG	[Housing]	941,049,507
OCFO	[Office of the Chief Financial Officer]	317,293,835
GNMA	[Gov't National Mortgage Assoc.]	10,000,000
REAC	(Real Estate Assessment Center]	8,700,000
FHEO	[Fair Housing and Equal Opportunity]	630,000
OCHCO	[Office of Chief Human Capital Officer]	7,079
PDR	[Policy Development and Research]	5,854
TOTAL		1,277,686,275

Figure 2. Key Strengths and Weaknesses of the HUD Privacy Program

While HUD has improved certain aspects of its privacy program, it faced challenges in establishing a program commensurate with its extensive holdings of sensitive information.

Since our last privacy program evaluation in 2014, HUD prioritized the privacy program by realigning it under a senior advisor to the Secretary, however, we learned that the person who occupied the position will be reassigned with no identified replacement. HUD had improved its privacy impact assessment and documentation processes, and took a more active role to ensure privacy is properly addressed in the agency's technology and business operations. However, HUD had not established a strategic plan for privacy, and many key initiatives were put on hold pending the staffing of key privacy program management positions. HUD had not integrated privacy risks into its enterprise risk management (ERM) process, had not formalized many compliance and oversight practices, and had still not been able to fully identify and inventory its extensive holdings of PII. Figure 2 lists key strengths and weaknesses identified during the evaluation of the HUD privacy program.

Strengths

- *Increased priority and organizational support for the privacy program*
- *Increasing collaboration between the privacy and IT programs*
- *Increased participation in agency decisions by the senior privacy official*
- *Pockets of privacy expertise across the agency*
- *Strong privacy impact assessment process*
- *More active role by privacy staff in system development life cycle*
- *Strong general privacy awareness training for all employees*

Weaknesses

- *No strategic plan or Chief Privacy Officer to guide program initiatives*
- *Lack of a formal compliance program*
- *Incomplete inventory of PII*
- *Improper retention of PII within some applications, in violation of National Archives and Records Administration records retention requirements*
- *Privacy risks not integrated into the ERM program*
- *Inconsistent communications and collaboration*
- *Inconsistent specialized privacy training for privacy staff*

Table of Contents

Introduction

Objective

The overall objective of this evaluation was to determine the effectiveness of the U.S. Department of Housing and Urban Development (HUD) privacy program and practices. Specific objectives included:

- Evaluate the adequacy of HUD privacy strategies, plans, policies, and procedures to meet Federal laws, regulations, and guidance, with focus on the framework of Federal requirements set forth in Appendix B
- Assess the implementation and enforcement of privacy procedures, processes, and controls across HUD in terms of completeness, consistency, and appropriateness.
- Assess HUD program governance in terms of organizational structure, sufficiency and placement of personnel, expertise of key staff, sufficiency of resources, level of executive support, and any other governance issues discovered during the evaluation.
- Determine if HUD established procedures, measures, and automated mechanisms to verify its privacy control effectiveness.
- Assess progress made subsequent to our 2014 privacy program evaluation.

Background

HUD is entrusted with the personal information of tens of millions of Americans. An effective HUD privacy program is essential to meeting the agency's responsibility to properly protect personally identifiable information (PII). OIG last conducted an evaluation of the HUD privacy program in 2014. Subsequent to that evaluation:

- Multiple OIG evaluations have found weaknesses regarding the security of HUD information systems and the personal information housed in those systems.

- The privacy program relocated from the Office of the Chief Information Officer (OCIO) to the Office of Administration in 2015, and three different individuals have served as the Senior Agency Official for Privacy (SAOP) within the past 3 years.

- The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued updated requirements and guidance for Federal agency privacy in the past 2 years.

- Multiple breaches of Federal information systems have heightened the need for agencies to assess their privacy practices and strengthen the security of their systems.[1]

[1] Examples include the compromise of sensitive background investigation records of more than 20 million individuals through an Office of Personnel Management system https://fcw.com/articles/2018/03/07/opm-breach-

Recent breaches of information systems in both the public and private sector have prompted Congress to place heightened priority on modernizing and properly securing Federal information systems to protect sensitive data, including PII. In January, 2017, OMB issued updated requirements for preparing and responding to a breach of PII.[2] The head of each agency is ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within the agency. Each agency is required to designate a SAOP, who is responsible for oversight of the agency's privacy program.[3] HUD designated a senior advisor to the Secretary as the agency SAOP, and the Privacy Office is located under the Executive Secretariat within the Office of Administration (OA). As required under the Federal Information Security Modernization Act (FISMA), the SAOP submits the annual report to OMB on the status of the agency privacy program.

Federal SAOPs are expected to work closely with other agency officials to ensure an effective privacy program. For example, it is critical that the SAOP work with the agency procurement staff to ensure that privacy requirements and concerns are incorporated into contracts. It is also imperative that the SAOP and Chief Information Officer (CIO) collaborate to ensure that privacy protection requirements are built into the system development life cycle, and that the most effective technical protections are available to fully identify and protect the PII maintained by the agency. Similarly, the SAOP must be enabled to work closely with the enterprise risk management (ERM) program to ensure that critical risks are promptly identified and elevated to senior leadership with the same priority as any other mission risk facing the agency.

Numerous statutes, regulations, and guidelines govern the treatment and handling of PII by Federal agencies. A compendium of these key criteria are contained in Appendix B.

Scope and Methodology

The scope of this review was agency-wide, resulting in conclusions and recommendations made at the Department level. To accomplish our objective, we inspected agency policies and procedures, evaluated the level of implementation of these requirements by agency components, and assessed the privacy controls and practices in place for a representative subset of HUD information systems. Appendix C contains the full description of our scope and methodology.

---

contracting-oversight.aspx, and the breach of personal data of over 700,000 taxpayers through an IRS system in 2015 https://www.identityforce.com/blog/2017-data-breaches

[2] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

[3] OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy

Findings

1.0 Program Governance

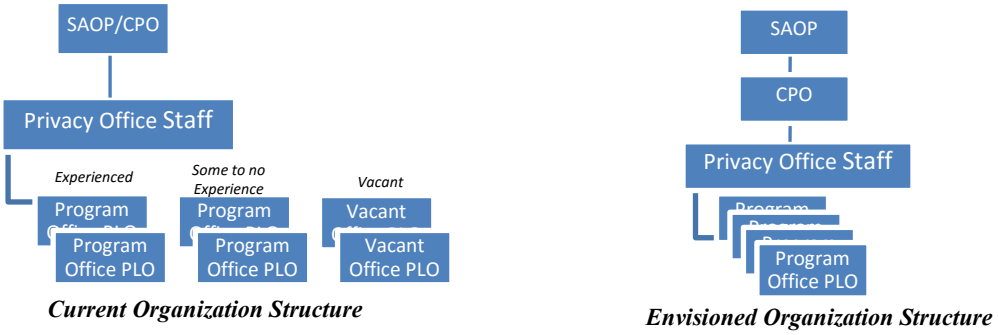
Key Findings:

- *The SAOP was a political appointee and senior advisor to the Secretary, participated in senior leadership decisions, and was focused on maturing the HUD privacy program.*
- *The SAOP was planning a workforce assessment to address skill and resource gaps.*
- *The Privacy Office was realigned under the Executive Secretariat, and better integrated with the Freedom of Information Act (FOIA) and Records Management Offices.*
- *Increased collaboration occurred with OCIO during the IT system development and system authorization processes.*
- *After approximately 6-8 months in the position, the current SAOP will be reassigned without an identified replacement.*
- *HUD lacked a strategic plan and Chief Privacy Officer to guide the privacy program.*
- *The program had not developed performance measures to assess program effectiveness.*
- *The program was not integrated with key enterprise programs such as risk management.*
- *The Privacy Office and stakeholders across the Department needed better training, communication, and collaboration.*

1.1 Privacy Program Structure and Alignment

The structure and alignment of the Privacy Office is critical to proper stewardship of the public's information, and is a fundamental building block of a robust privacy program. According to the Federal CIO Council Privacy Committee, "the success of an organization's privacy program is dependent upon its leadership."[4] HUD's current privacy organization consisted of the SAOP (who also served as the Chief Privacy Officer), Privacy Office staff, and privacy liaison officers (PLO) with varied experience in each program office, although the PLO position was vacant in some program offices. The envisioned organization will include a CPO in addition to the SAOP and trained program office PLOs in each program office, as shown in Figure 3.

Figure 3. HUD Privacy Program Organization Structure - Current vs. Envisioned



[4] Best Practices: Elements of a Federal Privacy program V 1.0, June 2010, https://www.energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf

Senior Agency Official for Privacy

The Privacy Office was led by the SAOP, who is the designated privacy steward for the Department. At the time of our interviews, the SAOP had been in the position for approximately 3 months and also served as the Chief Privacy Officer (CPO). However, prior to finalizing this report, we were notified that the SAOP would be reassigned and vacating the position without an identified replacement. Unlike in prior years, the new SAOP was a political appointee and had several roles including Senior Advisor to the Secretary, Director of the Executive Secretariat, and Correspondence Branch Chief. The current alignment of the SAOP aligns with recommended best practices.[5] The SAOP was engaged and involved in weekly senior leadership meetings where he is able to raise privacy issues to the attention of senior leadership and champion privacy related efforts. During our last evaluation, the lack of influence with senior leadership was a condition that negatively impacted the success of HUD's privacy program. The current SAOP was working directly with senior leadership and had begun to effect improvements to the privacy program. The program's future successes may be at risk until the SAOP and other key program positions are filled.

The Senior Agency Official for Privacy (SAOP) was a political appointee having a voice with senior leadership.

The SAOP had begun to effect improvements, but we were notified of a pending reassignment to a competing agency priority without a planned replacement.

Since our last evaluation in 2014, HUD's Privacy Office moved from the OCIO to the Office of Administration in the Executive Secretariat. HUD made this realignment after years of frequent organization restructuring within the OCIO and the Privacy Office, and indecision as to where the Privacy Office was best placed. The realignment of the Privacy Office under the Office of Administration improves integration between the Privacy, Records Management, and FOIA offices, with all of these offices now under the purview of the Executive Secretariat.

Privacy Office

The Privacy Office went through several staffing changes since the last OIG evaluation in 2014. Most of the staff were relatively new and had been in their positions for less than 2 years. The office is comprised of four program analysts and two IT security specialists. OIG provided a prior recommendation that HUD evaluate staffing requirements for its Privacy Office. At the time of this report, the SAOP was planning to staff a separate CPO position[6] and complete a workforce assessment that would determine the staff and resource levels necessary to fulfill HUD's considerable responsibility for protecting its PII.

Privacy Liaison Officers

Each program office in HUD designated PLOs who work with the Privacy Office and are responsible for ensuring that their offices are in compliance with agency and Federal privacy requirements. During our interviews, we noted that the level of knowledge and time dedicated

[5] Best Practices: Elements of a Federal Privacy program V 1.0 "The SAOP/CPO must be an integral member of the organization's senior management team so that she or he has both the authority and vantage point from which to develop, implement, and lead the Privacy program."

[6] OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy provides guidance for SAOPs to use discretion in staffing positions that can provide privacy leadership in support of the SAOP.

by PLOs towards privacy activities varied widely among the program offices, and direct privacy experience was limited. See *Figure 4* and *Figure 5*.

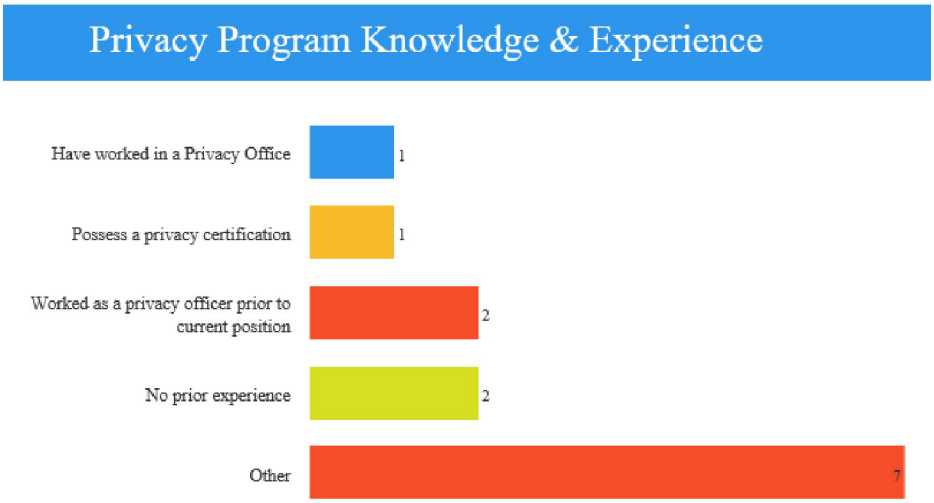


Figure 4. Extent of HUD Privacy program Knowledge and Experience

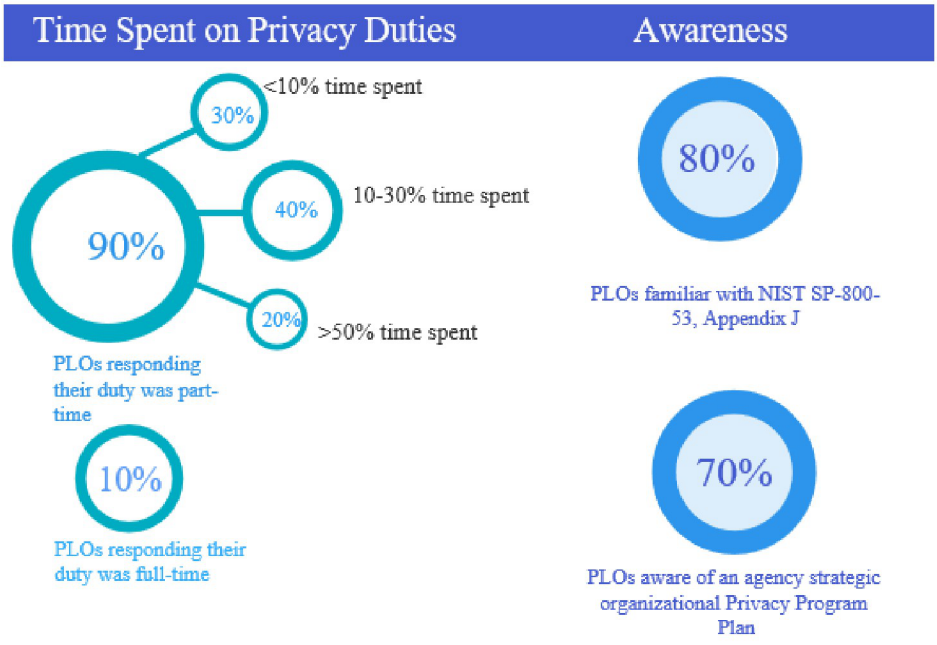


Figure 5. Summary of PLO time spent on privacy duties and awareness

Privacy Liaison Officer roles and responsibilities were unclear

PLOs play a key role in facilitating the implementation of privacy policy, documentation, and efforts across the organization. However, some individuals listed as PLOs were not familiar with the PLO title or were not aware that privacy tasks were their assigned duty. The latest PLO list included individuals who had retired, left the agency, did not perform that duty, or were not aware of their assigned role. Within the Office of Administration, the listed PLO was incorrect

and a new PLO was assigned a few days prior to the interviews we conducted. Many PLOs expressed a need for clarity on their responsibilities.

HUD had not established performance measures for many personnel tasked with privacy responsibilities, making it difficult to track accountability for its privacy program. For example, performance plans for many staff tasked with privacy roles and responsibilities, including the SAOP, did not include privacy elements. The SAOP had made it a priority to address this omission and reported that efforts were underway to update all pertinent personnel performance plans to include privacy elements.

1.2 Sources of Authority and Compliance Enforcement

Executive Support

According to Federal Government best practice,[7] "to be effective, the SAOP/CPO should have support from the head of the organization and the authority necessary to implement privacy policy for the organization and be involved in key decisions, projects and operations. Tangible and visible actions by the organization head attest to the importance of a vibrant privacy program. Support from the organization head may include: making it clear to subordinate officials that privacy issues are integral to the organization's accomplishing its mission; communicating the importance of privacy to the organization's staff; participating in selected privacy programs and initiatives; and providing adequate funding to support a robust privacy program."

The SAOP had direct communication with the Secretary and other senior officials to advise and champion privacy initiatives throughout the agency. However, while some program office personnel were aware of the SAOP, others were not aware or expressed uncertainty as to the permanence of the SAOP. HUD policy was also in need of updates, as the current HUD IT Security Handbook continued to list the SAOP and privacy program as part of the OCIO rather than the Executive Secretariat.

OMB further directed agencies to ensure that the SAOP have "the necessary authority at the agency to lead and direct the agency's program and carry out the privacy-related functions described in law and OMB policies."[8] We found no evidence that HUD had issued any formal notice communicating the new organizational structure and authority of the realigned SAOP and Privacy Office.

Strategic Planning

The planning process for HUD's privacy program was ad hoc. Efforts to prioritize projects and develop long term initiatives were essentially on hold, pending the hiring of a CPO with sufficient privacy experience. The privacy program's strategic plan was in draft and no timeline existed for its approval and circulation. While privacy was incorporated into the project

---

[7] Best Practices: Elements of a Federal Privacy program V 1.0, June 2010, https://www.energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

[8] OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.

planning and management (PPM) and authority to operate (ATO) processes, it was not closely integrated with HUD's strategic plan, mission, or risk management process at the enterprise level. This observation is a repeat from our 2014 evaluation.

HUD's Privacy program was not tied to HUD's strategic plan, mission or risk management process.

Compliance Program

In 2016, OMB formally assigned the SAOP with responsibility for establishing policy and facilitating the agency's privacy compliance efforts.[9]

HUD had not yet established performance measures and standards necessary for a formal privacy compliance program. HUD also had not established an effective directives process, another key element of an effective compliance program. The lack of a directives system is addressed in further detail in Section 2.2.

HUD's Privacy Office did not have a formal compliance program.

The lack of a privacy compliance program is a repeat finding from our 2014 evaluation. However, we observed evidence of recent compliance initiatives. The Privacy Office had implemented a more rigorous review process to ensure program offices completed required privacy documentation, and established a report format to keep the SAOP informed of privacy activities and project status. Program offices were required to post up-to-date privacy documents in the Cyber Security Assessment and Management (CSAM) application as part of the ATO process. Some program offices had also initiated their own internal compliance monitoring requirements and schedules. The Privacy Office monitored documentation for each system, provided up to 6 months' notice to system representatives regarding deadlines, and reviewed each artifact for approval. However, based on program office responses from our privacy liaison survey, compliance document recertification was done only when new systems were developed or modified or when ATOs needed to be renewed. To ensure effective privacy compliance, document review must be an ongoing task conducted in tandem with an effective continuous monitoring program.

1.3 Integration and Communication Across the Enterprise

Integration with Enterprise Programs

Protecting privacy is a core consideration for every federal organization, and it is best achieved when it is an integral part of the organization's business operations.[10] While we observed increased involvement by the privacy program in some agency activities, HUD's privacy program had not adequately integrated itself into the overall agency and business missions. For example, HUD's privacy program had not established repeatable processes for reviewing business operations, agency on-line activities, regulations, and contracts for potential privacy risks and impact.

---

[9] OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.

[10] Best Practices: Elements of a Federal Privacy program V 1.0, June 2010, https://www.energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

Two programs play especially important roles in the successful integration of privacy into agency business operations: information technology, to enhance systems and technologies for strengthening privacy protections, and ERM, to ensure proper identification and prioritization of privacy risks into agency risk decisions.

Information Technology (IT): The Privacy Office's level of interaction and integration with IT operations and security improved since the last review. The Privacy Office understood and had a more direct role in the ATO process. They had full access to review all systems security and privacy documentation and a formal approval role in the system authorization process. The staff participated as a key member on integrated project teams, took part in weekly project management meetings as necessary, and played a key role in the PPM process. Through a joint effort, the OCIO and Privacy Office implemented and were managing an enterprise email data loss prevention solution.

Interaction and integration between the OCIO and the Privacy Office had improved

However, there was limited participation by the Privacy Office during the system design and requirement specification phases of the system development process. The OCIO recommended privacy staff become more involved in the system design process to ensure privacy safeguards and controls are fully incorporated into the technical specifications for each new information system. At the time of this report, the SAOP and OCIO planned to continue and expand the collaboration between the Privacy Office and the OCIO.

Enterprise Risk Management: The privacy program was not yet integrated with HUD's ERM program because HUD's ERM program was only recently established. The Chief Risk Officer was aware of this deficiency, noting that privacy risk was not reported as a top agency risk despite the significant PII data that HUD maintained. The Enterprise Risk Officer planned to collaborate with the SAOP in the near future to address this deficiency within the ERM program.

Privacy risks were not included in HUD's ERM process

Communication with Program Offices

It is essential to integrate the privacy program in all facets of the organization by collaborating with key individuals. These individuals should include but are not limited to the CIO, Chief Information Security Officer (CISO), Enterprise Risk Officer, FOIA Officer, Personnel Security Office, Chief Financial Officer (CFO), Information System Security Officer's (ISSO), Paperwork Reduction Act (PRA) Liaison, Records Management Officer (RMO), legal counsel, website administrators, business owners, program officials, and system developers.

In addition to improving communications between the Privacy Office and IT operations and security, the Privacy Office reported improved coordination with the Office of General Counsel, though it was ad hoc. Also, regular conversations with staff from program offices occurred, as did quarterly meetings with the Records Management and FOIA offices. However, some program offices stated that information was not consistently communicated from the Privacy Office. The SAOP stated a goal for the program is to be more proactive and assert a stronger leadership role to ensure the Privacy Office is better integrated in privacy related matters across the agency.

Communication between the Privacy Office and program offices can be improved

The Privacy Office primarily communicated through email. The office agreed that changes could be made to better communicate across the agency. For example, a SharePoint dashboard exists, which was not shared outside the Privacy Office, and privacy reports were not provided to program office senior leadership on a regular basis. From the program office perspective, PLOs were not aware of steps and timelines for documents to be reviewed and returned and the Privacy Office had no established forum to communicate with PLOs as a group.

A data steward advisory group (DSAG) was cited during our interviews, which had been in existence for at least 5 years. However, the Privacy Office was not an active participant in the group. The Privacy Office could leverage the DSAG or lead a similar group to improve communication across the agency on privacy issues and share ideas and best practices.

1.4 Resources

OMB directed agencies to properly identify and plan resources necessary to meet legal requirements and carry out Federal privacy policies.[11] Such planning must consider the volume, sensitivity, and uses of PII by the agency. Given that HUD maintains a considerable volume of PII, used both internally and by business partners, it is critical that the agency properly resource its privacy program.

Budget

Privacy program success requires increased funding

Adequate funding and staff is integral for the SAOP/CPO to establish a mature privacy program.[12] A dedicated budget for initiating and implementing privacy initiatives did not exist, based on our discussion with the Privacy Office. The Privacy Office stated they were doing as much as reasonably could be expected with limited funding resources.

Additional budget would strengthen HUD's privacy protection by enabling the acquisition of technical solutions and contract support to address the critical need to completely identify, minimize, and protect its PII holdings. The Privacy Office also identified future initiatives that required funding and staff: acquiring a solution to create a more useful dashboard for keeping management apprised of privacy activities and risks; bolstering staff training (only one staff member had a Certified Information Privacy Professional /Government (CIPP/G) certification); providing PLO training; and launching a privacy awareness campaign.

Staffing

Privacy Office staff numbers fluctuated between three and eight people over the past 10 years. At the time of this evaluation, six full-time employees staffed the Privacy Office. The Privacy Office had not completed a workforce assessment to determine necessary staffing levels. The SAOP agreed that this assessment was needed to determine if the current staffing level was

---

[11] OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.

[12] Best Practices: Elements of a Federal Privacy program V 1.0, June 2010, https://www.energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

appropriate for accomplishing program goals and whether pay grades and levels of responsibility were congruent with the expertise required for current and future tasks. The SAOP intended to hire an experienced career CPO to lead the workforce assessment effort. In addition to hiring a CPO, the SAOP was planning to hire a supervisory or lead Privacy Officer to oversee the daily management of the privacy staff.

Recommendations - Program Governance

1. Ensure the privacy program is staffed with experienced personnel (such as a Chief Privacy Officer) to manage the operational aspects of the program.
2. Issue a notice at the Secretary level delegating and clarifying the authority and responsibilities of the SAOP and Privacy Office.
3. A. Document the roles and specific responsibilities of all positions assigned privacy responsibilities. B. Communicate these responsibilities on a recurring basis, at least annually, to individuals holding these positions.
4. Implement thorough human capital processes to ensure execution of the HUD privacy program and all its requirements.
5. Finalize and approve the draft privacy program strategic plan.
6. Ensure the privacy program is integrated with the enterprise risk program and that privacy risks are incorporated into the agency risk management process.
7. Establish an executive leadership dashboard to communicate continuous monitoring of key program risks and issues.
8. A. Develop an internal privacy program communication plan to describe how privacy issues will be disseminated and best practices will be shared. B. Implement the communication plan.
9. Develop a dedicated budget to address Privacy Office training needs and initiatives.

2.0 Policy, Procedures and Guidance

Key Findings:

- *HUD made significant improvements in oversight and monitoring of privacy documentation required for the information system authorization process.*
- *The Privacy Office issued an improved Privacy and Civil Liberties Impact Assessment template and guide.*
- *HUD established an effective privacy awareness training program for all employees, but did not have a specialized training program for personnel with privacy responsibilities.*
- *The privacy program could not rely on an effective directives system to issue enterprise requirements for privacy compliance.*
- *Some content in HUD privacy policy and procedures were outdated.*

2.1 Adequacy in Meeting Federal Requirements

HUD developed new processes that improved its oversight of privacy documentation

In 2013, NIST established mandatory privacy controls to be implemented for Federal information systems. [13] HUD had successfully incorporated these controls into its formal system authorization process. However, assessments were completed only when new systems were developed or modified or when systems were re-authorized every 3 years. HUD had yet to implement an effective continuous monitoring program.

Some key HUD privacy policy and guidance was outdated

HUD had established policy and procedures that addressed most Federal privacy requirements, and had also replaced its privacy impact assessment (PIA) process with a more rigorous privacy and civil liberties impact assessment (PCLIA) process. The Privacy Office was also leveraging various resources, such as those provided through the Federal Privacy Council, to keep abreast of current Federal privacy trends and requirements.[14] However, some agency privacy guidance was outdated. Both the HUD Privacy regulations and its Privacy Handbook were issued in 1995 and did not include newer privacy requirements. For example, the HUD Privacy Handbook did not include requirements for collection, use, and protection of PII. HUD had also not established procedures to meet key reporting requirements, such as an annual report submitted to OMB on computer matching programs. Section 3 below provides further discussion of specific documentation associated with implementing Privacy Act requirements.

We also noted that HUD had focused most of its guidance and oversight efforts on electronic records. The Privacy Office and some program offices expressed concern that non-electronic records need increased maintenance and security oversight. However, within HUD headquarters offices, the Privacy Office had recently overseen the conversion of a significant volume of paper records to electronic format.

2.2 Distribution of Guidance

Program office personnel reported that agency requirements and guidance continued to be issued by memorandums and email, making it difficult for offices to identify and track requirements, deliverables, and deadlines. This lack of rigor also hindered SAOP and Privacy Office efforts to establish accountability and efficiently determine the status of documentation submissions.

The Privacy Office had not established a formal process for issuing guidance.

During our review, we noted the absence of an effective HUD directives system. A proper directives system is an essential communication tool for meeting National Archives and Records Administration (NARA) requirements to document and track agency decisions and guidance. Given that the SAOP lacks line authority over

[13] NIST Special Publication 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J.
[14] https://www.fpc.gov/

program office personnel, including PLOs, a formal directives and compliance process, backed by senior agency leadership, is essential to HUD's enforcement of both Federal privacy requirements and Federal records requirements. In the absence of an effective agency directives system, the Privacy Office would benefit from creating its own formal process to establish firm privacy requirements and deadlines for PLOs and program offices.

The privacy office had established an internal website to communicate privacy guidance to program offices. However, PLOs reported that the website did not include all guidance and reference materials they needed to meet their privacy responsibilities and information was not timely posted.

Evidence of inconsistent work flow processes existed, which at times caused confusion and duplication of effort. For example, when preparing privacy documentation during the system authorization process, communications between program offices and the Privacy Office sometimes bypassed the PLOs, creating work flow complications and redundancy.

2.3 Privacy Program Training

HUD had a large and diverse set of stakeholders who used HUD's PII data, including employees, contractors, and third parties, such as lenders, appraisers, and public housing authorities. HUD employees consistently received annual privacy awareness training. The privacy training was included as a separate module of the overall mandatory IT Security awareness training suite. Privacy Office and program office staff reported improved content from prior years. The training addressed critical concerns, such as authorized collection of PII, sharing of PII with third parties, and the consequences of unauthorized use by any party. HUD also provided privacy training to large numbers of business partners, such as Housing Counseling Agency personnel.

All employees complete basic annual Privacy training

HUD had not developed a role-based training program for its specialized privacy employees.[15] As a result, PLOs and other staff with privacy roles were encouraged to seek training from outside vendors. The Privacy Office staff completed a privacy training boot camp and some PLOs had historically received specialized privacy training. HUD planned to develop and provide training specific to PLOs in 2018; the Privacy Office last provided such training in 2015. One program office required its entire staff to take additional privacy training. HUD had also applied lessons learned from actual incidents to further train staff on precautions that may prevent future similar incidents.

HUD had not established a specialized training program for personnel with key privacy responsibilities.

HUD did not have a consistent privacy training process for contractors. Some program offices reported that third parties and contractors instituted their own Privacy training. Other program offices were unsure if contractors completed any training. Only one program office tracked the completion of privacy training for its contractors. HUD required all third parties handling PII to

[15] NIST Special Publication 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, p J-9.

enter a formal agreement, such as a Memorandum of Understanding, that alerts the third party of proper PII handling requirements and the HUD incident response process. Contract agreements also contained privacy requirement clauses, and non-disclosure agreements were used as necessary.

Recommendations – Policy, Procedures and Guidance

10. Update all privacy guidance to reflect current Federal requirements and processes.
11. Implement a formal process for the Privacy Office to issue and communicate privacy guidance, requirements, and deadlines.
12. Update and continue to maintain a central collaboration area to include all current privacy program policies, procedures, and guidance.
13. Establish standard processes to ensure consistent work flow and communications between program office and Privacy Office personnel.
14. Ensure role-based privacy training is provided to all personnel with privacy responsibilities.
15. Ensure privacy awareness training is provided to all contractor and third party personnel.

3.0 Implementing and Documenting Privacy Act Requirements

Key Findings:

- *The Privacy Office improved its oversight of agency privacy activities and documentation.*
- *HUD implemented an improved privacy impact assessment process.*
- *Inconsistencies in the completion and documentation of Privacy Act Systems of Records Notices existed.*
- *HUD had not formalized its process to meet requirements for proper accounting of disclosures made under the Privacy Act.*

Federal statutes and policies establish privacy standards to properly identify and reduce activities having negative privacy impacts, and to notify the public how their information is protected and used. Key processes to ensure compliant protections include issuing Privacy Act Statements and completing PIAs, Privacy Act System of Records Notices (SORNs), and Computer Matching Agreements (CMA). HUD maintains this privacy documentation within its CSAM application.

3.1 Privacy Policy and Privacy Act Statements

Privacy Act statements inform individuals, at the time their information is collected, as to the legal authority and purpose of the collection and how the information will be used. Privacy Act statements also notify individuals if the information request is mandatory or voluntary, and the consequences of failing to provide information. Privacy Act statements are included on HUD forms when collecting PII data; HUD does not collect personal information verbally. The Privacy Office was in the process of reviewing all Privacy Act statements as part of the system authorization process.

HUD did not meet OMB requirements for maintaining an up-to-date central privacy program page[16] on its agency internet site. The HUD privacy page did not provide direct listings of, or links to, agency privacy documentation such as PIAs, SORNs, and CMAs. We also encountered at least one publicly accessible HUD website that did not reference the principle agency privacy program page as OMB requires. Some uncertainty among program offices existed as to whether Privacy Act statements were consistently included on all websites.

3.2 Privacy Impact Assessments

A PIA is a tool for identifying and assessing privacy risks throughout the life cycle of a program or system. Section 208 of the E-Government Act of 2002 requires Federal agencies to conduct PIAs for information systems that will collect personal information prior to system development or procurement. The Act also mandates a PIA be conducted when an IT system is substantially revised. A PIA describes the collected PII and explains how that information is maintained, protected, and shared. A PIA must analyze and describe:

- Whether the information collection complies with privacy-related legal and regulatory requirements regarding what information is collected, why the information is collected, the intended use of the information, and the proper sharing of the information;
- The risks and effects of collecting, maintaining, and disseminating the PII;
- Protections and processes for handling information to mitigate any potential privacy risks; and
- Options and methods for individuals to provide consent for the collection of their PII.[17]

HUD implemented a more robust privacy impact assessment process

HUD improved its privacy impact assessment process by implementing a more detailed PCLIA template to replace its PIA template. HUD also improved its tracking processes to ensure that all impact assessments underwent a formal review, and that all required documentation was completed and timely for each information system containing PII. HUD also initiated a privacy threshold assessment (PTA) template to replace its initial privacy assessment (IPA) template. PTAs were used to determine whether a system contained PII and therefore a PCLIA would be required for the system.

With one exception, each system we reviewed had completed a PCLIA. The OCIO had not completed a PCLIA for the Unisys Mainframe General Support System. The OCIO stated that general support systems constitute a platform, rather than an application that collects data, and that impact assessments had been completed only for the applications that are housed on the platform. However, the CIO and SAOP planned to determine if HUD should complete impact assessments for general support systems to assess privacy impact at the infrastructure level.

[16] OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services.
[17] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

3.3 System of Record Notices

A SORN is a notice published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose of the system, the authority for maintenance of the records, the categories of records maintained, the categories of individuals about whom records are maintained, and the routine uses to which the records are subject.[18]

The Privacy Office maintains an internal list of agency SORNs and assists program offices with reviews and updates. A search of HUD's websites provided a listing of SORNs by program office. SORN updates were required for material changes; however, the Privacy Office was uncertain whether all program offices issued updated SORNs when modifications were made to the system, such as an expansion of the types of information maintained or the manner in which the information is indexed or retrieved. Some program offices stated they issued updated SORNs, while others did not.

We noted inconsistencies between SORN documentation and system descriptions.

A review of IT system artifacts in CSAM revealed most systems identified as having PII had SORNS. In some cases, CSAM listed a system as not containing PII, yet a SORN and a PIA each described the PII collected. In other cases, CSAM listed a system as containing PII, yet no SORN existed and the PTA indicated no PII was being collected. As recommended in our 2014 evaluation, HUD needs to ensure it implements a recurring schedule and process for conducting SORN reviews; HUD also needs to ensure CSAM correctly reflects which systems contain PII.

HUD published procedures and contacts within their SORNs for private individuals to access their PII maintained in HUD systems of records and request corrections if necessary. The FOIA office is to process any requests for information that were submitted under the Privacy Act, tracking and managing such requests through its FOIA management system – FOIA Express, which had built-in privacy requirement capabilities. However, the FOIA staff were not specifically trained and were not actively capturing Privacy Act exemptions in FOIA Express.

3.4 Computer Matching Agreements

Computer matching agreements govern the recipient agency's use of information and procedures regarding notification to individuals, information verification, record retention, and data security. HUD used CMAs with business partners and third party users for information sharing purposes. HUD had a Data Integrity Board that included the SAOP, General Counsel, and CIO, which reviewed and approved CMAs. However, at the time of our interviews, HUD had not submitted its annual CMA report for 2017 as required by OMB Circular A-108. The Privacy Office had requested an extension from OMB for the 2017 report and was able to meet tha extended deadline subsequent to our review.

[18] OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act.

3.5 Accounting of Disclosures

The Privacy Act requires agencies to keep an accurate accounting of each instance it discloses an individual's information to any person or another agency, including: (1) Date, nature, and purpose of each disclosure; and (2) Name and address of the person or agency to which the disclosure was made. Disclosures must be retained for the life of the record or 5 years after the disclosure is made, whichever is longer, and made available to the person named in the record upon request.[19] Organizations must properly maintain the accounting of disclosures and be able to provide them to persons named in those records upon request. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3).[20]

Accuracy in HUD's accounting of Privacy Act disclosures was questionable.

FOIA Office staff were assigned with processing Privacy Act requests and maintaining a proper accounting of disclosures. FOIA staff stated that accounting of disclosures are maintained in the FOIA Management System (FMS2), commonly referred to as FOIA Express. However, during a demonstration of the FOIA Express system, a query for all Privacy Act requests made during the past year netted zero results. On this basis, the accuracy of the accounting of disclosures records could be questioned. The FOIA Office stated that requests were only classified as Privacy Act requests if the requestor identified the request as a Privacy Act request. The FOIA Office did not perform quality assurance checks to ensure that requests were properly identified. During our interviews, the FOIA Office acknowledged a potential lack of understanding of accounting of disclosure requirements and exceptions under the Privacy Act. As an anomaly, one program office stated that it maintained electronic copies of all disclosures separate from the FOIA Office and retained them for of 5 years.

Recommendations – Documentation and Handling of Privacy Information

16. Provide personnel tasked with handling Privacy Act requests with recurring training on Privacy Act exceptions.
17. Establish documentation procedures for accounting of disclosures made under the Privacy Act, as required by 5 USC 552a(c).
18. Establish an annual computer matching activity reporting process to meet the requirements of OMB Circular A-108.
19. Determine if general support system privacy threshold assessments or privacy impact assessments should be completed; if not, document the rationale.

[19] NIST Special Publication 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J.
[20] The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k).

4.0 Inventory

Key Findings:

- *HUD had not compiled an inventory of all the PII it maintains and lacked a technical solution to continually identify all PII in its possession.*
- *HUD's PII minimization efforts stalled, although some offices successfully continued initiatives to remove or mask PII within information systems.*
- *PII was retained indefinitely in some applications, in violation of NARA records retention requirements.*
- *Program offices identified systems containing PII; however, official documentation within CSAM did not identify all of these systems as containing PII.*

4.1 Inventory of Systems Containing Personally Identifiable Information

HUD had not identified all of its systems that contain PII

HUD had not developed an inventory of agency information systems that contain PII. HUD uses two applications to track and document its information systems. The Inventory of Automated Systems (IAS) lists all systems, but does not include a PII identifier. The CSAM application references which systems contain PII; however, CSAM does not include minor applications or describe data. The Privacy Office acknowledged that identifying minor applications containing PII is an ongoing problem. In fact, the accuracy of the overall HUD system inventory was subject to reliability and accuracy questions. A review of HUD web applications OIG conducted in 2017 determined that some web applications were unknown to the OCIO and were not included in either IAS or CSAM.

4.2 Identification of all Holdings[21] of Personally Identifiable Information

HUD was not able to identify and inventory all PII maintained within its environment, including both electronic and manual (e.g., paper) records. Our survey of HUD program offices revealed that HUD maintained over one billion records[22] of PII within its information systems alone. This amount was potentially duplicated to over two billion records due to mirroring of servers at separate data centers. Prior OIG reports have determined that HUD does not have an accurate inventory of all information systems to include all minor applications and defined authorization boundaries. An incomplete listing of information systems would preclude the development of a comprehensive inventory of PII holdings.

HUD lacked the capability to determine the amount and location of sensitive data on its information systems

In addition, HUD had not developed the technical capability or a process to identify and inventory PII holdings housed within various locations, such as shared drives, common file folders, databases, internal web locations, and data repositories. HUD also had not classified or labeled its sensitive data to enable the tracking and monitoring of data flow and data access. HUD had not recently required

[21] 'Holdings' refers to all instances of PII held by the agency in electronic or paper format.
[22] There may be multiple records for an individual.

HUD offices to conduct PII inventories of electronic and paper records. While inventory initiatives had been conducted in the past, most program offices reported the Privacy Office had not recently requested PII inventory information and no periodic reviews of PII holdings existed.

Without an accurate accounting of its PII holdings, HUD was unable to meet certain Federal privacy requirements, such as minimizing its overall holdings of PII. Lack of inventories also meant HUD was unable to assess the level of risk associated with both electronic and paper records, prioritize its security requirements, and apply controls commensurate with that risk to properly protect its PII holdings.

HUD completed a PCLIA for each major application as part of its system authorization process. The PCLIA lists the types of PII maintained in each major application. These documents provide one source of PII information that would assist HUD in developing a proper PII inventory.

4.3 Personally Identifiable information Minimization

HUD initiated an agency-wide effort in 2014 to minimize PII within its environment. The Privacy Office had not prioritized this effort in recent years due to limited resources, but planned to renew its efforts for PII minimization in FY 2019. Proper funding and renewed backing at the enterprise level by the SAOP will be essential to ensure expanded success in minimizing PII within the HUD environment. However, an agency-wide effort to minimize PII would be dependent on HUD's ability to identify and inventory all of its PII.

Nevertheless, several program offices had continued with individual initiatives to remove, mask, or anonymize PII within some of its applications. For example, one program office discontinued the collection of Social Security numbers (SSN) for use in a major application and was working to remove all SSNs from the system. Other offices had exhibited similar success or were in the process of developing tools to remove or mask PII. However, some offices reported their efforts to minimize PII were limited by budget constraints, technical limitations, or other priorities.

Some offices had successfully minimized their collection and use of PII

Some applications retained PII indefinitely, in violation of NARA retention requirements

Program offices reported less success in properly retaining PII within its applications in accordance with an approved records retention schedule. In some cases, records disposal was not addressed until an upgrade occurred or until storage reached capacity, which then forced the office to take action. Some applications were configured to archive and retain data within the application, including PII, indefinitely rather than removing data in compliance with the HUD records retention schedule. At least one application was designed to completely prevent the removal of case data; a significant and costly system modification would be required to resolve this issue. In addition, when systems were decommissioned, no process was in place for program offices to report destruction of records, including PII. One official stated, "There is not and never has been a consistent method of tracking destruction of records at HUD." The Records Officer was working with the program offices to address these gaps in HUD records retention practices.

Agencies must also minimize PII within their system testing environments. If PII is used in the test environment, it must be protected at the same level it is protected in the production environment.[23] Anonymizing the data removes this concern. HUD had not developed a policy on this issue, but reported that it uses only anonymized or randomly generated data for testing purposes. The Privacy Office planned to develop a policy that ensures techniques are used to minimize privacy risks when using PII in research, testing, or training.

Recommendations – Inventory

20. Develop the technical capability to identify, inventory, and monitor the existence of PII within the HUD environment.
21. Develop and implement a process to inventory all agency PII holdings not less than annually. [Dependent upon completion of Recommendation 20]
22. Renew the PII minimization effort, to include a prioritization by the SAOP of specific minimization initiatives.
23. Require all system owners to review the records retention practices for each information system and take any corrective actions necessary to ensure adherence to the applicable records retention schedule.

5.0 Safeguarding Privacy Information

Key Findings:

- *HUD had recently updated both its Breach Notification Response Plan and its HUD Incident Response plan.*
- *The Privacy Office had a more active role in the system authorization process.*
- *Physical protection measures for protecting sensitive information improved at headquarters offices, although HUD still lacked a clean desk policy.*
- *Communication procedures between the breach handling team and incident response team were not fully effective during a recent breach.*
- *HUD had not conducted inspections or assessed implementation of privacy controls at contractor or partner facilities such as lenders or public housing authorities.*

5.1 Physical Safeguards

HUD improved the physical security of its sensitive information at its Headquarters offices

HUD had not yet developed and implemented a formal "clean desk" policy. However, a brief inspection at headquarters offices revealed that HUD had taken measures since our last review in 2014 to improve the physical security of its sensitive records. Most personnel were provided locking cabinets as part of an office refresh and locked centralized filing areas were observed. We found no sensitive information left unattended at fax machines or printers and, with few exceptions, workstations were notably absent of sensitive documents.

[23] NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Section 4.2.4.

Without conducting additional inspections, we were unable to determine if security measures improved consistently across all HUD offices. Due to resource limitations, the Privacy Office staff did not conduct inspections of physical security measures in HUD field offices. In response to our survey, several PLOs reported that some physical security measures were typically in place at their office, including key card access for buildings, file rooms, and work areas; locked file cabinets; Privacy Act labeling; and secure printer locations. However, no evidence existed that program offices formally reported these measures to the Privacy Office. As a result, the Privacy Office was unable to ascertain the level of physical security in place for sensitive data within agency facilities.

The Privacy Office did not conduct inspections of physical security at field offices.

For some programs offices, it was routine business practice to receive sensitive data on removable media, such as compact disks, that were mailed to HUD by external business partners. While the offices reported the media was destroyed after the data were loaded to the system, this process created risks that were not directly addressed by the Privacy Office or OCIO.

5.2 Incident Response and Handling

HUD recently updated its Breach Notification Response Plan and successfully executed the plan multiple times in recent years. The OCIO recently modified its incident response procedures to include specific processes and contacts for incidents involving privacy data. However, OCIO personnel did acknowledge they were unaware of a prior significant breach in which HUD ended up providing credit monitoring for affected individuals. HUD also acknowledged it had not developed a metric to measure the estimated cost of a potential breach. This prevents HUD from accurately determining the risk posed to the agency by a compromise of its sensitive data. Without this information, it is difficult to properly prioritize privacy controls and incident response processes in the overall agency mission and business processes.

HUD made improvements educating users on proper communications for reporting IT security and PII incidents. Reporting procedures were posted on the HUD privacy webpage, the general HUD webpage, and in security awareness training. However, the Privacy Office reported that it has been more difficult to establish consistent reporting procedures for business partners. Business partners do not have a direct incident reporting channel, and normally reported any issues to a HUD program office business point of contact, who then relayed the concern to the HUD Computer Incident Response Team (CIRT).

The Privacy Office was aware of and had implemented the latest breach notification requirements OMB issued.[24] The HUD CIRT worked closely with the U.S. Computer Emergency Response Team (U.S. CERT) to ensure proper implementation of breach notification procedures.

[24] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017.

HUD had limited capability to conduct incident trend analysis

Incidents were tracked and documented in the HUD Service Desk ticketing system. A specific queue was in place to route any tickets for potential privacy incidents to the Privacy Office staff. Weekly and monthly incident reports were provided to the Privacy Office. However, privacy staff reported that the ticketing system does not lend itself to robust trend analysis, and the Privacy Office was unaware of any agency that conducted incident trend analysis.

5.3 Oversight of Partner Organizations and Contractors

The Privacy Office had not conducted inspections of business partners or contractor offices or facilities, and reported a lack of capacity to implement such inspections. We determined that the OCIO conducted inspections of some contractor facilities, but the Privacy Office was not aware of such inspections and had not been provided results. Failure to conduct or coordinate such inspections precludes the Privacy Office from ascertaining the level of security in place at partner and contractor facilities. HUD had no process to verify that partner organizations and contractors complied with agency privacy policies and requirements.

Recommendations – Safeguarding Privacy Information

24. A. Issue a clean desk policy prohibiting unattended and unsecured sensitive data in workplaces. B. Implement procedures to enforce the clean desk policy.

Appendixes

Appendix A – Summary of Privacy Program Recommendations

OIG report	No.	Recommendation	Status
FY 2018 **Report Number: 2018-OE-0001**	1	Ensure the privacy program is staffed with experienced personnel (such as a Chief Privacy Officer) to manage the operational aspects of the program.	
	2	Issue a notice at the Secretary level delegating and clarifying the authority and responsibilities of the SAOP and Privacy Office.	
	3	A. Document the roles and specific responsibilities of all positions assigned privacy responsibilities. B. Communicate these responsibilities on a recurring basis, at least annually, to individuals holding these positions.	
	4	Implement thorough human capital processes to ensure execution of the HUD privacy program and all its requirements.	
	5	Finalize and approve the draft privacy program strategic plan.	
	6	Ensure the privacy program is integrated with the enterprise risk program and that privacy risks are incorporated into the agency risk management process.	
	7	Establish an executive leadership dashboard to communicate continuous monitoring of key program risks and issues.	
	8	A. Develop an internal privacy program communication plan to describe how privacy issues will be disseminated and best practices will be shared. B. Implement the communication plan.	
	9	Develop a dedicated budget to address Privacy Office training needs and initiatives.	
	10	Update all privacy guidance to reflect current Federal requirements and processes.	
	11	Implement a formal process for the Privacy Office to issue and communicate privacy guidance, requirements, and deadlines.	

	12	Update and continue to maintain a central collaboration area to include all current privacy program policies, procedures, and guidance.	
	13	Establish standard processes to ensure consistent work flow and communications between program office and Privacy Office personnel.	
	14	Ensure role-based privacy training is provided to all personnel with privacy responsibilities.	
	15	Ensure privacy awareness training is provided to all contractor and third party personnel.	
	16	Provide personnel tasked with handling Privacy Act requests with recurring training on Privacy Act exceptions.	
	17	Establish documentation procedures for accounting of disclosures made under the Privacy Act, as required by 5 USC 552a(c).	
	18	Establish an annual computer matching activity reporting process to meet the requirements of OMB Circular A-108.	
	19	Determine if general support system privacy threshold assessments or privacy impact assessments should be completed; if not, document the rationale.	
	20	Develop the technical capability to identify, inventory, and monitor the existence of PII within the HUD environment.	
	21	Develop and implement a process to inventory all agency PII holdings not less than annually. [Dependent upon completion of Recommendation 20]	
	22	Renew the PII minimization effort, to include a prioritization by the SAOP of specific minimization initiatives.	
	23	Require all system owners to review the records retention practices for each information system and take any corrective actions necessary to ensure adherence to the applicable records retention schedule.	
	24	A. Issue a clean desk policy prohibiting unattended and unsecured sensitive data in workplaces. B. Implement procedures to enforce the clean desk policy.	
FY 2014	1	Establish and approve an organizational structure for HUD's Privacy Office.	Closed

Report Number: 2014-OE-0003	2	Evaluate the staffing requirements for the approved Division, including adequate funding and qualified resources	Open
	3	Solidify executive leadership for the privacy program and assure the Senior Agency Official for Privacy (SAOP) and the Departmental Privacy Officer have the necessary qualifications and expertise.	Closed
	4	Issue a privacy directive outlining an organizational approach to proper handling of PII, to include establishing accountability of managers for their employees' understanding of privacy protection requirements and the penalties for non-compliance.	Open
	5	Clarify HUD policy to establish CSAM as the authoritative [information] system inventory. **[Repeat Finding – Rec. 57, 2013-ITED-0001]**	Closed
	6	Develop and execute a plan, process, and schedule that will ensure timely completion of an accurate and complete inventory of all PII holdings as required by OMB M-07-16, to include all sources and forms of PII held by the agency, including electronic and non-electronic.	Closed
	7	Issue a formal directive requiring timely research and feedback by the Program Offices to the Privacy Office to ensure completion of the PII inventory; hold managers accountable for timely response by their office.	Open
	8	Develop or procure, and implement, a solution that enables scanning and detection of PII on any and all network and computer resources.	Open
	9	Establish and enforce a single incident reporting Helpdesk; document and disseminate clear instruction for all users; and educate all users on proper incident reporting procedures. **[Repeat Finding – Rec. 14, 2013-ITED-0001]**	Closed
	10	Update and issue Incident Response and Reporting policies and procedures, including privacy breach response standard operating procedures.	Open
	11	Align the DLP solution management within existing continuous monitoring processes.	Open
	12	Educate and train all users, including external business partner on proper recognition and reporting of incidents, to include specific training regarding potential PII incidents, such as PII breaches.	Closed
	13	Conduct annual training for all HBNRT members on their roles and responsibilities for all aspects of PII incident handling, including but not limited to preparation, risk analysis, escalation, notification, and mitigation.	Closed

	14	Establish and formally approve SORN guidance.	Closed
	15	Complete the ongoing project to review and update existing SORNs, including a master reconciliation between system inventory and SORNs.	Closed
	16	Establish a schedule and procedures for conducting mandated SORN reviews in a recurring and timely manner.	Open
	17	Conduct a quality review and update of all SORN data in CSAM; establish procedures and assign responsibilities to ensure data is properly maintained.	Open
	18	Complete the ongoing project to review and update existing IPAs and PIAs, including a master reconciliation between system inventory, PIAs and SORNs; prioritize all PIAs that were completed on an outdated PIA template.	Open
	19	Establish a schedule and process for ensuring PIAs reviews are conducted in a recurring and timely manner.	Open
	20	Engage executive leadership to formalize the authority and assign sufficient resources to complete a proper inventory of PII holdings in both electronic and non-electronic form and re-invigorate efforts to reduce PII holdings.	Closed
	21	Establish a repeatable process, including a master repository, to ensure collection and maintenance of accurate PII inventory data.	Open
	22	Re-invigorate efforts, including support from executive leadership, to eliminate the unnecessary and unwarranted use of Social Security Numbers.	Closed
	23	Identify and formally inventory all CMAs in effect within HUD.	Closed
	24	Assure CMAs are regularly reviewed and updated, and confirm HUD's compliance with the safeguarding and data management requirements.	Closed
	25	Conduct a risk assessment of CMA agreements to determine risks to the agency and develop mitigation strategies.	Closed
	26	Develop incident response and notification procedures specific to data involved in CMAs.	Closed
	27	Establish and fully implement a privacy training program in accordance with federal guidance. **[Repeat Finding – Rec. 23, 2013-ITED-0001]**	Closed
	28	Provide proper privacy training throughout the organization to ensure that staff understands the proper handling of sensitive data including PII, and their responsibilities in protecting such information. Training	Closed

		must include awareness training for all personnel and specialized training for personnel with specific roles and responsibilities regarding Privacy. **[Repeat Finding – Rec. 49, 2013-ITED-0001]**	
	29	Establish clear responsibilities and assignments for development and delivery of all mandatory privacy training. Privacy training can be stand-alone or integrated with IT Security training.	Closed
	30	Develop and implement a process to oversee and ensure that all HUD partners who access or handle PII are provided proper privacy training commensurate with their role.	Closed
	31	Develop a plan to enhance expertise within the Privacy Office staff, to include specialized training for personnel with key responsibilities.	Closed
	32	Conduct a risk assessment of physical security measures in place at HUD in order to determine HUD's current physical security posture, identify its vulnerabilities, and implement safeguards to mitigate risk.	Open
	33	Establish a formal internal reporting mechanism, including input from a privacy compliance program, to keep executive leadership informed on the current status of the agency privacy program, progress of its initiatives, and any outstanding risks associated with privacy.	Open
	34	Develop a repeatable process for gathering complete and verifiable information to arrive at an accurate SAOP report, with accountability for timely input from program offices.	Open

Appendix B – List of Federal Privacy Criteria

The Privacy Act of 1974, 5 U.S.C. § 552a, as amended by the Computer Matching and Privacy Protection Act of 1988.

The Privacy Act imposes various requirements for Federal agencies whenever they collect, create, maintain, and distribute records (as defined in the Act, and regardless of whether they are in hardcopy or electronic format) that can be retrieved by the name of an individual or other identifier. (As amended by the Computer Matching and Privacy Protection Act of 1988).

Broadly stated, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them. The Act focuses on four basic policy objectives:

(1) To restrict disclosure of personally identifiable records maintained by agencies;
(2) To grant individuals increased rights of access to agency records maintained on themselves;
(3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete; and
(4) To establish a code of "fair information practices" this requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The Act requires agencies to collect only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. Agencies are required to protect this information from any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained, and must not disclose this information except under certain circumstances.

The information collected is considered a record under the Privacy Act if it is an item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

When an agency has a group of any records under its control from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, the agency has a Privacy Act System of Records. The Privacy Act requires that a public notice, commonly referred to as a System of Records Notice (SORN), be published in the Federal Register that describes the existence and character of the system of records. In addition, the Privacy Act requires SORNs to include:

- The name and location of the system;
- The categories of individuals on whom records are maintained in the system;
- The categories of records maintained in the system;

- Each routine use of the records contained in the system, including the categories of users and the purpose of such use;
- The policies and practices of the agency regarding storage, irretrievability, access controls, retention, and disposal of the records;
- The title and business address of the agency official responsible for the system;
- The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
- The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
- The categories of sources of records in the system.

Computer Matching and Privacy Protection Act of 1988, and the Computer Matching and Privacy Protection Amendments of 1990

The Computer Matching and Privacy Protection Act of 1988, and the Computer Matching and Privacy Protection Amendments of 1990 concern the electronic sharing of information. These laws:

- Apply to automated systems of records when the information in the systems is shared between Federal or non-Federal agencies.
- Spell out the procedural requirements that agencies must follow when performing computer-matching activities.
- Require agencies to provide to individuals whose records are in matching systems the opportunity to receive notice and to refute adverse information before having a benefit denied or terminated.
- Require agencies which are engaged in matching activities to establish Data Integrity Boards to oversee computer-matching activities.

The provisions of these Acts have been incorporated into the following Sections of the Privacy Act (5 U.S.C. § 552a):

  - (a)(8)-(13);
  - (e)(12);
  - (o), (p), (q), (r), (u); and
  - 1994 & Supp.

OMB Circular A-130, Appendix 1

OMB Circular A-130, Appendix 1, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records about Individuals, describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act.

OMB Circular A-108

OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act supplements and clarifies existing OMB guidance, including OMB Circular

A-130. The circular addresses how government agencies review, report, and publish system of records notices and matching agreements; promotes collaboration through interagency review of government-wide systems of records notices; and outlines requirements for Privacy Act compliance reviews.

Federal Information Security Modernization Act of 2014

Under the Federal Information Security Modernization Act (FISMA), agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

FISMA requires each federal agency to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or source. Relative to the protection of privacy information, an effective information security program should include:

- Periodic assessments of risk
- Policies and procedures that are based on risk assessments, cost-effectively reduce security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each information system
- Security awareness training to inform personnel of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks
- Periodic (at least annual) testing of the effectiveness of policies, procedures, practices, and controls
- A process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies
- Procedures for detecting, reporting, and responding to security incidents

Paperwork Reduction Act of 1980 as amended by Paperwork Reduction Act of 1995

The Paperwork Reduction Act (PRA) is designed to reduce the paperwork burden placed by the Federal government upon individuals, private businesses, state and local governments, educational and nonprofit organizations, and others. Among other purposes, PRA is also intended to maximize the public benefits of information collected and used by the Federal government; improve the quality and use of Federal information to strengthen decision making, accountability and openness; coordinate Federal information resource management policies; and minimize agencies' costs of information creation and use.

Agencies must obtain OMB approval ("clearance") before collecting information from the public (defined as 10 or more "persons" (individuals, groups, associations, State or local government units, etc.) with various mechanisms including forms, questionnaires, and surveys.
PRA requires each agency to establish its own paperwork clearance process within the agency's Office of the Chief Information Officer and requires the process to be sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved. Agency reviews; public notice and comment; certification that the proposed collection

meets statutory requirements; and publication that the certification has been submitted must all be completed before undertaking a collection of information.

E-Government Act of 2002

Section 208 of the E-Government Act of 2002 (Public Law No. 107-347) requires agencies to:

(1) Conduct Privacy Impact Assessments (PIA) of information systems and collections and, in general, make PIAs publicly available.
(2) Post privacy policies on agency Web sites used by the public.
(3) Translate privacy policies into a machine-readable format.
(4) Report annually to the OMB on compliance with Section 208.

OMB Memorandum M-17-12

Preparing for and Responding to a Breach of Personally Identifiable Information sets forth the policy for Federal agencies to prepare for and respond to a breach of Personally Identifiable Information (PII). It includes a framework for assessing and mitigating risk and provides guidance on providing notification and services to individuals affected by a breach. This memorandum also implements recommendations included in OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government.

OMB Memorandum M-17-06

Policies for Federal Agency Public Websites and Digital Services updates policies regarding Federal agency public websites and digital services and requires that each agency ensure transparency by maintain a central privacy resource webpage on the agency's principal website. The agency's Privacy Program page must serve as a central source for information about the agency's practices with respect to PII.

OMB Memorandum M-16-24

Role and Designation of Senior Agency Officials for Privacy provides the authority and responsibilities of the Senior Agency Official for Privacy (SAOP), and lays out requirements for agencies to identify and plan for the financial, human, information, and infrastructural resources necessary for the position to carry out the privacy-related functions described in law and OMB policies.

OMB Memorandum M-03-22

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, particularly section 208. The guidance urges agencies to conduct reviews of how IT is used to collect information about individuals or when agencies develop or buy new IT systems to handle collections of IIF (Information in an Identifiable Form).

This memo defines a PIA as an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. PIAs must analyze and describe the following:

- What information is to be collected (e.g., nature and source);
- Why the information is being collected (e.g., to determine eligibility);
- Intended use of the information (e.g., to verify existing data);
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose);
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
- How the information will be secured (e.g., administrative and technological controls);
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a; and
- What choices the agency made regarding an IT system or collection of information as a result of performing the PIA. PIAs must also be approved by a "reviewing official" and be made publicly available to the extent that they do not contain classified or sensitive information or raise security concerns.

OMB Memorandum M-06-16

Protection of Sensitive Agency Information includes a checklist for agency use for protecting PII that is remotely accessed or transported outside the agency. The checklist is based on NIST SPs 800-53, Recommended Security Controls for Federal Information Systems; and 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (Second Public Draft). In addition, M-06-16 recommends the encryption of all data on mobile computers/devices that carry sensitive data, two-factor authentication for remote access, "time-out" functions for remote access and mobile devices, and the logging of all computer-readable data extracts from databases containing sensitive information.

OMB Memorandum M-14-04

Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management provides instructions for meeting agency FY2013 reporting requirements under the FISMA and includes instructions on agency privacy program management.

NIST Special Publication 800-122:

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) provides guidelines for implementing a risk-based approach to protecting PII in the context of information security. It recommends a process that involves identifying the PII that an agency holds, classifying the PII by confidentiality impact level, and providing safeguards based on the confidentiality impact level. It also provides recommendations for developing an incident response plan.

NIST Special Publication 800-53 Rev 4, Appendix J:

Security and Privacy Controls for Federal Information Systems and Organizations (Appendix J: Privacy Control Catalog) provides a structured set of privacy controls based on best practices; establish a linkage between privacy and security controls for purposes of enforcing privacy and security controls which may overlap in concept and implementation; demonstrates the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls; and promotes closer cooperation between privacy and security officials within the federal government to help achieve the objectives of senior leaders/executives in enforcing the federal privacy requirements. Controls are structured similar to the security controls within SP 800-53, and are intended for use primarily by the agency SAOP and CIO. Controls in the appendix are based on the Fair Information Practices Principles embodied in the Privacy act of 1974, Section 208 of the E-Government Act of 2002, and the OMB policies described above.

Appendix C – Scope and Methodology

We performed this evaluation to determine the effectiveness of U.S. Department of Housing and Urban Development's (HUD) Privacy program and practices as of April 30, 2018. The scope of this review was agency-wide, resulting in conclusions and recommendations made at the Department level.

This evaluation was conducted in accordance with the Quality Standards for Inspection and Evaluation, issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions. To accomplish our objective, we conducted the following activities:

- An inspection of strategies, plans, policies, procedures, practices, and standards established by the HUD Office of Administration, Office of the Chief information Officer (OCIO), Office of the Chief Procurement Officer, and other agency components determined to play key roles in the issuance of agency Privacy guidance.
- An inspection of Privacy procedures and practices as implemented and in use at Headquarters Program Offices.
- An assessment of the Privacy controls and practices for a representative subset of six HUD information systems, to determine the adequacy of protection afforded the PII that is collected, maintained, used, or disseminated by these systems.

The team conducted the evaluation at three levels:

Agency Level - We gained an understanding of the agency Privacy-related policies and guidance HUD established. We compared program policies, procedures, and practices to the applicable Federal laws and criteria to determine the overall compliance with the current Federal Privacy requirement framework at the agency level. This step included interviews with the Senior Agency Official for Privacy (SAOP) and representatives for the Privacy Office, OCIO, Freedom of Information Act Office, and Records Management Office.

Component Level - We gained an understanding of the extent to which HUD offices have properly implemented law, Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) Guidance, and agency Privacy policies and procedures. This step included site visits, interviews, and documentation reviews at the Program Office level, including interviews with several Privacy Liaison Officers (PLO) assigned to the Program Offices.

Information System Level - We gained an understanding of the extent to which HUD information systems have properly implemented and documented privacy protection requirements. This step included an evaluation of a representative subset of information systems, and included site visits, interviews, and documentation reviews at the Program Office level. Interviews included System Owners, PLOs, Information System Security Officers, and others.

Evaluation techniques included:

- Development and use of a Fieldwork Program Guide for interviews, with questions based on key Federal Privacy program criteria (Appendix B);
- Issuance of a Survey to the Privacy Liaison Officer located in each Program Office, with results compiled into one document for analysis;
- Inquiries with management, program, systems, and general personnel;
- Inspection of documentation and artifacts related to the implementation of Privacy requirements, including documentation contained within the HUD Cyber Security Assessment and Management (CSAM);
- Site visits to agency offices, to gain an understanding of information security, privacy, and data protection programs and practices, as well as to further evaluate the implementation of all Privacy requirements;
- Comparison of Privacy data, artifacts, and practices with relevant agency and Program Office policy and processes, as well as OMB and NIST criteria;

We evaluated the implementation of Privacy practices, policies, and procedures at specific HUD offices, focusing on a representative sample set of agency information systems.

Table 3: Representative sample of information systems

SAMPLE	IAS ID	PROGRAM OFFICE	SYSTEM NAME	ACRONYM	PII	SECURITY CATEGORIZATION	TYPE
1	P181	PIH/ REAC	Enterprise Income Verification	EIV	Y	MODERATE C-Mod I- Mod A-Mod	Major
2	F17	HSG Single Family	Computerized Home Underwriting Management System	CHUMS	Y	MODERATE C-Mod I- Mod A-Mod	Major
3	A43	HSG Finance and Budget	Single Family Insurance System	SFIS	Y	MODERATE C-Mod I- Mod A-Mod	Major
4	A67	OCFO	Line of Credit Controls System	LOCCS	Y	MODERATE C-Mod I- Mod A-Mod	Major
5	P212	OCIO	Mainframe (UNISYS)	UNISYS	N	MODERATE C-Mod I- Mod A-Mod	General Support System
6	P113	PIH	PIH Inventory Management System	PIH-IMS	Y	MODERATE C-Mod I- Mod A-Low	Major

Source: HUD CSAM system, IAS

Program Offices:

- Office of Public and Indian Housing (PIH): The PIH mission is to ensure safe, decent, and affordable housing; create opportunities for residents' self-sufficiency and economic independence; and assure the fiscal integrity of all program participants.
- Office of the Chief Information Officer (OCIO): OCIO enables delivery of HUD programs, services, and management processes by providing high-quality information, technology solutions, and services.
- Office of Housing (HSG): HSG single family (SF) provides affordable homeownership and refinancing opportunities to individuals and families by making home loans more readily available through the single family housing mortgage insurance programs. SF programs insure mortgage lenders against losses from default, enabling lenders to provide mortgage financing on favorable terms to homebuyers.
- Real Estate Assessment Center (REAC): REAC provides and promotes the effective use of accurate, timely, and reliable information assessing the condition of HUD's portfolio; provides information to help ensure safe, decent, and affordable housing; and restores the public trust by identifying fraud, abuse, and waste of HUD resources.
- Office of Housing – Finance and Budget: Provides support to all Office of Housing components.
- Office of the Chief Financial Officer (OCFO): OCFO prepares, justifies, and monitors the budget including responding to OMB and congressional concerns and questions related to appropriations law; establishes and maintains financial systems; develops internal control programs and addresses material weaknesses in the Department; produces audited consolidated financial statements; and processes accounting transactions and payments.

Appendix D – List of Abbreviations and Acronyms

ACRONYM	DEFINITION
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CPO	Chief Procurement Officer
CSAM	Cybersecurity Assessment and Management
DIAMS	digital identity and access management system
DLP	data loss prevention
ERM	enterprise risk management
FHEO	Fair Housing and Equal Opportunity
FISMA	Federal Information Security Modernization Act
FTE	full-time employee
FY	fiscal year
GAO	U.S. Government Accountability Office
GNMA	Government National Mortgage Association
HSG	Office of Housing
IAS	inventory of automated systems
IG	inspector general
IPT	integrated project team
ISCM	information security continuous monitoring
ISSO	information system security officer
IT	information technology
NARA	National Archives and Records Administrative
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OCPO	Office of the Chief Procurement Officer
OITS	Office of Information Technology Security
OMB	Office of Management and Budget
PCLIA	privacy and civil liberties impact assessment
PDR	Policy Development and Research
PII	personally identifiable information

ACRONYM	DEFINITION
PIV	personal identity verification
POA&M	plans of actions and milestones
PTA	privacy threshold assessment
REAC	Real Estate Assessment Center
SAOP	Senior Agency Official for Privacy
SLA	service-level agreement
SOP	standard operating procedure
SORN	system of record notice
SP	special publication
SSN	Social Security number

Appendix E – Agency Comments and OIG Response

Program Office Comments

The Office of Administration concurs with the report and the included 24 HUD OIG recommendations as written, and has elected to provide no comments.

OIG's Response to Program Office Comments

The Office of Evaluation has accepted the agency's concurrence with this report, and will continue to work with the agency toward development and approval of corrective action plans for each recommendation provided herein.

Appendix F - Acknowledgements

This report was prepared under the direction of Brian T. Pattison, Assistant Inspector General for Evaluation, and John Garceau, Director of the Information Technology Evaluation Division (iTED). The Office of Evaluation staff members who contributed are recognized below.

Major Contributors

Tamara Jones, Management Analyst
Adam Bernstein, Information Security Specialist
Isaiah Bellais, Information Security Specialist
Craig Wood, Information Security Specialist

The Office of Inspector General is an independent and objective oversight agency within the U.S. Department of Housing and Urban Development. We conduct and supervise audits, evaluations, and investigations relating to the Department's programs and operations. Our mission is to promote economy, efficiency, and effectiveness in these programs, while preventing and detecting fraud, abuse, and mismanagement.

Report fraud, waste, and mismanagement in HUD programs and operations by

Completing this online form: https://www.hudoig.gov/report-fraud
Emailing the OIG hotline: hotline@hudoig.gov
Faxing the OIG hotline: (202) 708-4829

Sending written information to

U.S. Department of Housing and Urban Development
Office of Inspector General Hotline (GFI)
451 7th Street SW, Room 8254
Washington, DC 20410

Whistleblowers are protected by law.

https://www.hudoig.gov/fraud-prevention/whistleblower-protection

Website

https://www.hudoig.gov/

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
OFFICE OF EVALUATION
Information Technology Evaluations Division

Report number: 2018-OE-0001