Senior Agency Official For Privacy

2021

Annual Report

Department of Housing and Urban Development

Section 1: General Privacy Program Requirements

1a. Has the head of the agency designated a Senior Agency Official for Privacy (SAOP), as required by Executive Order 13719 and OMB guidance?

Yes

1b. Has the agency reported the name, title, and contact information of the current SAOP to OMB on the MAX website of the Federal Privacy Council? (Indicate "N/A" if the agency has not designated an SAOP.)

Yes

1c. Does the SAOP have the necessary position, expertise, and authority to serve in the role of SAOP? (Select all that apply or indicate "N/A" if the agency has not designated an SAOP.)

- Position
- Expertise
- Authority

1d. Does the SAOP have the necessary role and responsibilities within the agency for each of the following? (Select all that apply or indicate "N/A" if the agency has not designated an SAOP.)

- Policy making
- Compliance
- Risk management activities

1e. Has the agency developed and maintained a privacy program plan?

Yes

1f. Does the agency's privacy program plan include a description of each of the following? (Select all that apply or indicate "N/A" if the agency has not developed and maintained a privacy program plan.)

- Structure of the privacy program
- Resources dedicated to the privacy program
- Role of the SAOP and other privacy officials and staff
- Strategic goals and objectives of the privacy program
- Program management and common controls in place or planned for meeting applicable privacy requirements and management privacy risks

Section 2A: Information Systems

Section 2A: Information Systems

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

Yes

Section 2B: Information Systems

2b. Number of information systems reported in response to question 1.1 of the FY 2021 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

		2b. Number of information systems reported in response to question 1.1 of the FY 2019 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable			2c. Number of information systems reported in question 2b that the agency authorized or reauthorized to operate during the reporting period.			2d. Number of information systems reported in question 2c where the SAOP reviewed and approved the categorization of the information system in accordance with NIST FIPS Publication 199 and NIST Special			2e. Number of information systems reported in question 2c where the SAOP reviewed and approved a system privacy plan for the information system prior to the information system's authorization or reauthorization.			2f. Number of information systems reported in question 2c where the SAOP conducted and documented the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented for the information system prior to the information			2g. Number of information systems reported in question 2c where the SAOP reviewed the information system's authorization package to ensure compliance with applicable privacy requirements and manage privacy risks, prior to the authorizing official making a risk		
Bureau/ Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
ADMIN	Submitted to Agency	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
CFO	Submitted to Agency	6	0	6	4	0	4	4	0	4	4	0	4	4	0	4	4	0	4
CPD	Submitted to Agency	3	0	3	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
CPO	Submitted to Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ODOC	Submitted to Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ENFC	Submitted to Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FHEO	Submitted to Agency	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GNMA	Submitted to Agency	0	6	6	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1

Section 2B: Information Systems

		2b. Number of information systems reported in response to question 1.1 of the FY 2019 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable			2c. Number of information systems reported in question 2b that the agency authorized or reauthorized to operate during the reporting period.			2d. Number of information systems reported in question 2c where the SAOP reviewed and approved the categorization of the information system in accordance with NIST FIPS Publication 199 and NIST Special			2e. Number of information systems reported in question 2c where the SAOP reviewed and approved a system privacy plan for the information system prior to the information system's authorization or reauthorization.			2f. Number of information systems reported in question 2c where the SAOP conducted and documented the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented for the information system prior to the information			2g. Number of information systems reported in question 2c where the SAOP reviewed the information system's authorization package to ensure compliance with applicable privacy requirements and manage privacy risks, prior to the authorizing official making a risk		
Bureau/ Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
HSG	Submitted to Agency	20	8	28	10	3	13	10	3	13	10	3	13	10	3	13	10	3	13
OCIO	Submitted to Agency	8	16	24	6	5	11	6	5	11	6	5	11	6	5	11	6	5	11
OGC	Submitted to Agency	2	0	2	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
OIG	Submitted to Agency	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDR	Submitted to Agency	2	1	3	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
PIH	Submitted to Agency	4	0	4	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2
REAC	Submitted to Agency	2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ODEEO	Submitted to Agency	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FPM	Submitted to Agency	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
Agency Totals		49	34	83	26	10	36	26	10	36	26	10	36	26	10	36	26	10	36

Section 3A: Information Technology Systems and Privacy Impact Assessments

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

Yes

Section 3B: Information Technology Systems and Privacy Impact Assessments

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

		3b. Number of IT systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a privacy impact assessment (PIA) under the E-Government Act of 2002.			3c. Number of IT systems reported in question 3b that are covered by an up-to-date PIA.		
Bureau/ Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
ADMIN	Submitted to Agency	1	0	**1**	1	0	**1**
CFO	Submitted to Agency	6	0	**6**	6	0	**6**
CPD	Submitted to Agency	3	0	**3**	3	0	**3**
CPO	Submitted to Agency	0	0	**0**	0	0	**0**
ODOC	Submitted to Agency	0	0	**0**	0	0	**0**
ENFC	Submitted to Agency	0	0	**0**	0	0	**0**
FHEO	Submitted to Agency	1	0	**1**	1	0	**1**
GNMA	Submitted to Agency	0	6	**6**	0	6	**6**
HSG	Submitted to Agency	20	8	**28**	20	8	**28**
OCIO	Submitted to Agency	8	16	**24**	8	16	**24**
OGC	Submitted to Agency	2	0	**2**	2	0	**2**
OIG	Submitted to Agency	0	1	**1**	0	1	**1**
PDR	Submitted to Agency	2	1	**3**	2	1	**3**
PIH	Submitted to Agency	4	0	**4**	4	0	**4**
REAC	Submitted to Agency	2	0	**2**	2	0	**2**
ODEEO	Submitted to Agency	0	1	**1**	0	1	**1**
FPM	Submitted to Agency	0	1	**1**	0	1	**1**
Agency Totals		49	34	**83**	49	34	**83**

Section 3C: Information Technology Systems and Privacy Impact Assessments

3d. Does the agency have a written policy for PIAs that includes each of the following? (Select all that apply or indicate "N/A" if the agency does not have a written policy for PIAs.)

- A requirement that a PIA be conducted and approved prior to the development, procurement, or use of an IT system that requires a PIA
- A requirement that system owners, privacy officials, and IT experts participate in conducting PIAs
- A requirement for PIAs to be updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks associated with the use of a particular IT system

3e. Does the agency have a process or procedure for each of the following? (Select all that apply.)

- Assessing the quality and thoroughness of each PIA
- Performing reviews to ensure that appropriate standards for PIAs are maintained
- Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated
- Ensuring that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks

Section 4: Systems of Records

4a. Number of Privacy Act systems of records maintained by the agency during the reporting period (including those operated by a service provider or a contractor on behalf of the agency).

74

4b. Number of Privacy Act systems of records reported in question 4a for which an up-to- date system of records notice (SORN) has been published in the Federal Register.

74

4c. Does the agency have a process for determining whether a new or revised SORN is required when the agency collects or maintains information about individuals?

Yes

4d. Does the agency have a process for each of the following? (Select all that apply.)

- Ensuring that information collections include a Privacy Act Statement, if required
- Receiving, processing, and responding to individuals' requests for access to and amendment of records in a system of records

Section 4: Systems of Records

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

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

Section 5: Considerations for Managing PII

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

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

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

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

Section 6: Social Security Numbers

Section 6: Social Security Numbers

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

Yes

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

Yes

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

Yes

6d. Does the written policy referred to in question 6c provide specific criteria to use when determining whether the collection or use of SSNs is necessary? (Indicate "N/A" if the agency does not have a written policy.)

Yes

6e. Does the written policy referred to in question 6c establish a process to ensure that any collection or use of SSNs determined to be necessary remains necessary over time? (Indicate "N/A" if the agency does not have a written policy.)

Yes

6f. Has the agency taken steps during the reporting period to eliminate the unnecessary collection, maintenance, and use of SSNs? (Indicate "N/A" if the agency has already eliminated all unnecessary collection, maintenance, and use of SSNs by the agency.)

Yes

Section 7: Digital Services

7a. Does the agency maintain an inventory of the following? (Select all that apply or indicate "N/A" if the agency does not maintained an inventory of any digital services.)

- The agency’s public websites

7b. In accordance with the E-Government Act of 2002 and OMB guidance, does the agency maintain and post privacy policies on the following? (Select all that apply or indicate "N/A" if the agency does not maintain any of the following)

Section 7: Digital Services

• The agency's public websites

7c. Does the agency have a process to regularly review and update the privacy policies for each of the following? (Select all that apply or indicate "N/A" if the agency does not maintained any of the following.)

• The agency's public websites

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

No

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

No

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

N/A

Section 8: Budget and Acquisition

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

Yes

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

No

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

No

Section 8: Budget and Acquisition

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

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

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

Yes

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

3

Section 9: Contractors and Third Parties

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

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

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

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

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

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

Section 9: Contractors and Third Parties

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

Yes

9e. Has the agency established rules of behavior, including consequences for violating rules of behavior, for contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

Yes

9f. Does the agency ensure that contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access (indicate "N/A" if the agency does not have established rules of behavior)?

Yes

Section 10: Workforce Management

10a. Does the agency ensure that the agency's privacy workforce has the appropriate knowledge and skill?

Yes

10b. Has the agency assessed its hiring, training, and professional development needs with respect to privacy during the reporting period?

Yes

10c. Has the agency developed a workforce planning process to ensure that it accounts for privacy workforce needs?

Yes

10d. Has the agency developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions?

Yes

Section 11: Training and Accountability

11a. Does the agency provide foundational privacy training to its Federal employees (including managers and senior executives)?

Section 11: Training and Accountability

Yes

11b. What percentage of the agency's Federal employees (including managers and senior executives) received foundational privacy training during the reporting period?[i] (Indicate "N/A" if the agency does not provide foundational privacy training.)

100%

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

Yes

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

100%

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

Yes

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

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

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

Yes

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

Yes

Section 11: Training and Accountability

Section 12: Incident Response

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

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

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

Yes

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

Yes

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

Yes

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

0

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

0

12g. How many breaches, as OMB Memorandum M-17-12 defines the term 'breach,' did the agency report to Congress as major incidents (as defined in OMB Memorandum M-20-04 and OMB Memorandum M-21-02) during the reporting period?

0

Section 12: Incident Response

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

N/A

Section 13: Risk Management Framework

13a. Has the agency implemented a risk management framework to guide and inform each of the following? (Select all that apply or "N/A" if the agency has not implemented a risk management framework.)

- Categorization of Federal information and information systems that process PII
- Selection, implementation, and assessment of privacy controls
- Authorization of information systems and common controls
- Continuous monitoring of information systems that process PII

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

Yes

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

Yes

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

Yes

Section 14: Privacy Program Website

14a. Does the agency have a Privacy Program Page located at (or redirected from) www.[agency].gov/privacy?

Yes

14b. Does the agency's Privacy Program Page include a list and provide links to complete, up-to-date versions of all agency SORNs? (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records.)

Yes

Section 14: Privacy Program Website

14c. Does the agency's Privacy Program Page include a list and provide links to all PIAs? (Indicate "N/A" if the agency does not maintain, operate, or use any IT systems that require a PIA.)

Yes

14d. Does the agency's Privacy Program Page include a list and provide links to up-to-date matching notices and agreements for all active matching programs in which the agency participates? (Indicate "N/A" if the agency does not participate in any matching programs.)

No

14e. Does the agency's Privacy Program Page include citations and provide links to the final rules published in the Federal Register that promulgate each Privacy Act exemption claimed for their systems of records? (Indicate "N/A" if the agency has not claimed any Privacy Act exemptions for their systems of records.)

N/A

14f. Does the agency's Privacy Program Page include a list and provide links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f)? (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records.)

Yes

14g. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency policies on privacy, including any directives, instructions, handbooks, manuals, or other guidance?

Yes

14h. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency reports on privacy?

No

14i. Does the agency's Privacy Program Page include instructions in clear and plain language for individuals who wish to request access to or amendment of their records pursuant to 5 U.S.C. § 552a(d)? (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records.)

Yes

14j. Does the agency's Privacy Program Page include appropriate agency contact information for individuals who wish to submit a privacy-related question or complaint?

Yes

Section 14: Privacy Program Website

14k. Does the agency's Privacy Program Page identify the agency's SAOP and include appropriate contact information for the SAOP's office?[i] (Indicate 'N/A' if the agency has not designated an SAOP.)

Yes