Senior Agency Official For Privacy (SAOP)

2025

FISMA Annual

Department of Housing and Urban Development

Section 1: General Privacy Program Requirements

1a Did the agency have a Senior Agency Official for Privacy (SAOP) designated by the head of the agency, as required by Executive Order 13719 and OMB guidance, for the duration of the reporting period? [1]

Yes

1b Did the agency ensure that the name, title, and contact information of the SAOP reported to OMB on the Connect.gov (formerly MAX.gov) website of the Federal Privacy Council remained up-to-date? [2]

Yes

1c The SAOP is required to have the necessary position, expertise, and authority to serve in the role. [3] Which of the following requirements were met? (Select all that apply.)

- Position
- Expertise
- Authority

1d For which of the following areas did the SAOP have the necessary role and responsibilities within the agency? [4] (Select all that apply.)

- Policy making
- Compliance
- Risk management

1e Did the agency maintain an up-to-date privacy program plan? [5]

Yes

1f For which of the following areas did the agency`s privacy program plan include a description? [6] (Select all that apply.)

- 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 controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks

[1] See Executive Order 13719, seealso OMB M-16-24, Role and Designation of Senior Agency Officials forPrivacy (Sept. 15, 2016).
[2]See OMB M-16-24, at 4.
[3]The role and requirements for the SAOP are described in OMB guidance. Seegenerally OMB M-16-24.
[4]See id. at 3-4.
[5]Each agency is required to develop and maintain a privacy program plan thatprovides an overview of the agency's privacy program, including a descriptionof the structure of the privacy program, the resources dedicated to the privacyprogram, the role of the SAOP and other privacy officials and staff, thestrategic goals and objectives of the privacy program, the program managementcontrols and common controls in place or planned for meeting applicable privacyrequirements and managing privacy risks, and any other information determinednecessary by the agency's privacy program. See OMB Circular No. A-130,app. I § 4(c)(2), (e)(1).

[6]See id. app. I § 4(c)(2).

Section 2A: Information Systems

2a Did the agency maintain an inventory of the agency`s information systems [7] that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII)? [8]

Yes

[7] The term “information system” means a discrete set ofinformation resources organized for thecollection, processing, maintenance, use, sharing,dissemination, or disposition of information. 44 U.S.C. § 3502(8). The term “information resources” means informationand related resources, such as personnel, equipment, funds, and informationtechnology. Id. § 3502(6). The term “Federal information system”means an information system used or operated by an agency or by a contractor ofan agency or by another organization on behalf of an agency. OMB Circular No.A-130, § 10(a)(23).
[8] See OMB Circular No. A-130, § 5(a)(1)(a)(ii). The term“personally identifiable information” means information that can be used todistinguish or trace an individual’s identity, either alone or when combinedwith other information that is linked or linkable to a specific individual. Id.§ 10(a)(57).

Section 2B: Information Systems

		2b. Number of information systems reported in response to question 1.1 of the FY 2024 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.			2c. Number of information systems reported in question 2b that the agency authorized or reauthorized to operate during the reporting period.[15]			2d. Number of information systems reported in question 2c where the SAOP reviewed and approved the categorization of the information system in accordance with OMB guidance, as well as NIST FIPS Publication 199 and NIST Special Publication 800-60.[16]			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.[17]			2f. Number of information systems reported in question 2c where the SAOP conducted and documented the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented for the information system prior to the information system's authorization or reauthorization.[18]			2g. Number of information systems reported in question 2c where the SAOP reviewed the information system's authorization package to ensure compliance with applicable privacy requirements and manage privacy risks, prior to the authorizing official making a risk determination and acceptance decision.[19]		
Bureau/Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
ADMIN	In Progress	1	2	3	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
CFO	In Progress	4	3	7	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
CPD	In Progress	3	2	5	2	0	2	2	0	2	2	0	2	2	0	2	2	0	2
FHEO	In Progress	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
GNMA	In Progress	0	3	3	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
HSG	In Progress	19	9	28	7	2	9	7	2	9	7	2	9	7	2	9	7	2	9
OCIO	In Progress	10	15	25	3	4	7	3	4	7	3	4	7	3	4	7	3	4	7
OGC	In Progress	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OIG	In Progress	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDR	In Progress	2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PIH	In Progress	11	3	14	2	1	3	2	1	3	2	1	3	2	1	3	2	1	3
FPM	In Progress	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ODEEO	In Progress	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OPA	In Progress	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Agency Totals		52	40	92	15	10	25	15	10	25	15	10	25	15	10	25	15	10	25

[9] “Authorization to operate” is theofficial management decision given by a senior Federal official or officials toauthorizeoperation of an information system and to explicitly accept the risk to agencyoperations (including mission, functions, image, or reputation), agency assets,individuals, other organizations, and the Nation based on the implementation ofan agreed-upon set of security and privacy controls. Id. app. I§ 4(d).
[10]See id. app. I § 4(a)(2), (e)(7).
[11]Agencies shall develop and maintain a privacy plan that details the privacycontrols selected for an information system that are in place or planned formeeting applicable privacy requirements and managing privacy risks, details howthe controls have been implemented, and describes the methodologies and metricsthat will be used to assess the controls. See id. app. I§ 4(c)(9), (e)(8).
[12]See id. app. I § 4(e)(3).
[13]See id. app. I § 4(e)(9).

Section 3A: Information Technology Systems and Privacy Impact Assessments

3a Did the agency maintain an inventory of the agency`s information technology [14] (IT) systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

Yes

[14]The term “information technology” means any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used inthe automatic acquisition, storage, analysis, evaluation, manipulation,management, movement, control, display, switching, interchange, transmission, or reception of data or information by theagency. See id. § 10(a)(45).

Section 3B: Information Technology Systems and Privacy Impact Assessments

		3b. Number of IT systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a privacy impact assessment (PIA) under the E-Government Act of 2002.			3c. Number of IT systems reported in question 3b that are covered by an up-to-date PIA.		
Bureau/Component	Submission Status	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
ADMIN	In Progress	1	3	4	1	3	4
CFO	In Progress	4	2	6	2	0	2
CPD	In Progress	3	2	5	0	2	2
FHEO	In Progress	1	0	1	1	0	1
GNMA	In Progress	0	3	3	0	0	0
HSG	In Progress	19	11	30	5	6	11
OCIO	In Progress	10	15	25	0	5	5
OGC	In Progress	1	0	1	0	0	0
OIG	In Progress	0	1	1	0	0	0
PDR	In Progress	2	0	2	0	0	0
PIH	In Progress	11	3	14	10	3	13
FPM	In Progress	0	1	1	0	1	1
ODEEO	In Progress	0	1	1	0	1	1
OPA	In Progress	0	0	0	0	0	0
Agency Totals		52	42	94	19	21	40

[15] Each agency is required to update PIAs whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology. For the purposes of this question, an up-to-date PIA is a PIA that reflects any changes to the information technology, changes to the agency's practices, or other factors that altered the privacy risks associated with the use of such information technology. See id. app. II § 5(e).
[16] See id.

[17]See id.
[18]See id.
[19]See id.
[20]See id.
[21]See id.

Section 3C: Information Technology Systems and Privacy Impact Assessments

3d Which of the following requirements were included in the agency`s written policy for PIAs? (Select all that apply.)

- A requirement for PIAs to be conducted and approved prior to the development, procurement, or use of an IT system that requires a PIA [23]
- A requirement that system owners, privacy officials, and IT experts participate in conducting PIAs [24]
- 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 [25]

3e For which of the following actions did the agency have a process or procedure? (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 What is the number of Privacy Act systems of records [22] maintained by the agency during the reporting period (including those operated by a service provider or a contractor on behalf of the agency)?

64

4b What is the number of Privacy Act systems of records reported in question 4a that were covered by up-to-date system of records notices (SORNs) published in the Federal Register? [23]

64

4c Did the agency have a process for determining whether a new or revised SORN is required when the agency collects or maintains information about individuals? [24]

Yes

4d For which of the following actions did the agency have a process? (Select all that apply.)

• Ensuring that information collections include a Privacy Act Statement, if required [32]
• Receiving, processing, and responding to individuals requests for access to and amendment of records in a system of records [33]

4e For which of the following requirements did the agency`select, implement, assess, and monitor privacy controls for information systems that contain information maintained in a system of records? (Select all that apply.)

• Systems of records include only information about an individual that is relevant and necessary to accomplish a purpose required by statute or executive order [34]
• SORNs remain accurate, up-to-date, and appropriately scoped [35]
• SORNs are published in the Federal Register [36]
• SORNs include the information, and are drafted in the format, required by OMB Circular No. A-108 [37]
• Significant changes to SORNs have been reported to OMB and Congress [38]
• Routine uses remain appropriate and the recipient s use of the records continues to be compatible with the purpose for which the information was collected [39]
• Each exemption claimed for a system of records pursuant to 5 U.S.C. 552a(j) and (k) remains appropriate and necessary [40]
• 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 the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees [41]
• 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 [42]

[22]The term “system of records” means a group of any records under the control ofany agency from which information is retrieved by the name of the individual orby some identifying number, symbol, or other identifying particular assigned tothe individual. 5 U.S.C. § 552a(5).
[23]Agencies are required to publish a SORN in the Federal Register whenestablishing a new system of records and must also publish notice in the FederalRegister when making significant changes to an existing system of records. Forthe purposes of this question, an up-to-date SORN is a published SORN thatreflects any significant changes that have been made to the system of records. OMB Circular No. A-108, § 6(a).
[24]See 5 U.S.C. § 552a(e)(4).
[25] See id. § 552a(e)(3).
[26]See id. § 552a(d).
[27]See id. § 552a(e)(1); OMB Circular No. A-108,§ 12(a).
[28]See 5 U.S.C. § 552a(e)(4); OMB Circular No. A-108, § 12(b).
[29]See OMB Circular No. A-108, § 12(b).
[30]See id.
[31]See 5 U.S.C. § 552a(r); OMB Circular No. A-108, § 12(b).
[32]See OMB Circular No. A-108, § 12(c).
[33]See id. § 12(d).
[34]See id. § 12(e).
[35]See id. § 12(f).

Section 5: Considerations for Managing PII

5a To what extent did the agency ensure that PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of was accurate, relevant, timely, and complete? [36] (Select one of the following.)

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

5b To what extent did 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? [37] (Select one of the following.)

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

[36]See OMB Circular No. A-130, § 5(f)(1)(e).
[37]See id. § 5(f)(1)(d).

Section 6: Social Security Numbers

6a Did the agency have an inventory of the agency`s collection, maintenance, and use of Social Security numbers (SSNs)? [38]

Yes

6b Did the agency maintain the inventory of SSNs referenced in question 6a as part of the agency`s inventory of information systems referenced in question 2a?

Yes

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

Yes

6d Did the written policy referenced in question 6c provide specific criteria to use when determining whether the collection or use of SSNs is necessary?

Yes

6e Did the written policy referenced in question 6c establish a process to ensure that any collection or use of SSNs determined to be necessary remains necessary over time?

Yes

6f Did the agency take steps to eliminate the unnecessary collection, maintenance, and use of SSNs? [39]

Yes

[38]Agencies are not required to have an inventory of collection, maintenance, anduse of SSNs. However, agencies need to have a sufficient evidentiary basis todetermine whether they have met the requirement to eliminate unnecessarycollection, maintenance, and use of SSNs. See id. § 5(f)(1)(f).
[39]Agencies are required to take steps to eliminate unnecessary collection,maintenance, and use of SSNs, and explore alternatives to the use of SSNs as apersonal identifier. Id.

Section 7: Digital Services

7a For which of the following digital services did the agency maintain an inventory? (Select all that apply.)

• The agency`s public websites

7b In accordance with the E-Government Act of 2002 and OMB guidance, [40] for which of the following digital services did the agency maintain and post privacy policies? (Select all that apply.)

• The agency`s public websites

7c For which of the following digital services did the agency have a process to regularly review and update the privacy policies? (Select all that apply.)

• The agency`s public websites

7d Did the agency have a written policy it developed and implemented for the agency`s use of social media?

Yes

7e Did the agency use web measurement and customization technologies on any website or mobile application? [41]

No

7f Did the agency review the use of web measurement and customization technologies to ensure compliance with all laws, regulations, and OMB guidance? [42]

N/A

[40]See id. § 5(f)(1)(j).
[41]See OMB M-10-22, Guidance for Online Use of Web Measurement andCustomization Technologies (June 25, 2010).
[42]See id.

Section 8: Budget and Acquisition

8a Did the agency identify and plan for the resources needed to implement the agency`s privacy program? [43]

Yes

Did the agency have a policy that includes explicit criteria for analyzing privacy risks when considering IT investments? [44]

8b

No

8b.1 Explanation

The agency is currently revising current policy to include privacy considerations for IT investments per OMB A-130.

8c 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? [45]

No

8c.1 Explanation

The agency is establishing a procedures to include SAOP into the review process per OMB A-130.

8d To what extent did the agency plan and budget to upgrade, replace, or retire any information systems that maintain PII for which protections commensurate with risk could not be effectively implemented? [46] (Select one of the following.)

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

8e Did the agency ensure that, in a timely manner, the SAOP was made aware when information systems and components that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII could not be appropriately protected or secured? [47]

Yes

8f What is the 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 could not be appropriately protected or secured?

1

[43]See OMB Circular No. A-130, app. I § 4(b)(1).
[44]See id. § 5(d)(3).
[45]See id. § 5(a)(3)(e)(ii).
[46]See id. app. I § 4(b)(3).
[47]See id. app. I § 3(b)(10).

Section 9: Contractors and Third Parties

9a To what extent did 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 incorporated privacy requirements and were sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information? [48] (Select one of the following.)

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

9b To what extent did the agency, consistent with the agency`s authority, ensure that the requirements of the Privacy Act applied to a Privacy Act system of records when a contractor operated the system of records on behalf of the agency to accomplish an agency function? [49] (Select one of the following.)

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

9c To what extent did the agency ensure appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information? [50] (Select one of the following.)

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

9d Did the agency maintain a mandatory agency-wide privacy awareness and training program for all contractors? [51]

Yes

9e Did the agency have 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? [52]

Yes

9f Did the agency ensure that contractors have read and agreed to abide by the rules of behavior referenced in question 9e prior to being granted access? [53]

Yes

[48]See id. § 5(a)(1)(b)(ii); id. app. I § 4(j)(1).
[49]See id. app. I § 4(j)(3).
[50]See id. app. I § 4(j)(2)(a).
[51]See id. app. I § 4(h)(1), (4)-(5).
[52]See id. app. I § 4(h)(6).
[53]See id. app. I § 4(h)(7).

Section 10: Workforce Management

10a Did the agency ensure that the agency`s privacy workforce has the appropriate knowledge and skill?

Yes

10b Did the agency assess its hiring, training, and professional development needs with respect to privacy? [54]

Yes

10c Did the agency have a workforce planning process to ensure that it accounts for privacy workforce needs? [55]

Yes

10d Did the agency have a set of competency requirements for privacy staff, including program managers and privacy leadership positions? [56]

Yes

[54]See id. § 5(c)(6).
[55]See id. § 5(c)(1).
[56]See id.

Section 11: Training and Accountability

11a Did the agency maintain a mandatory agency-wide privacy awareness and training program for all Federal employees? [57]

Yes

11b What percentage of Federal employees participated in a mandatory agency-wide privacy awareness and training program during the reporting period? [58]

100%

11c Did the agency provide role-based privacy training to Federal employees with assigned privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties? [59]

No

11c.1 Explanation

The agency Privacy Office is developing role-based/specialized privacy training for Federal employees handling PII before authorizing access to Federal information or information systems or performing assigned duties.

11d What percentage of Federal employees with assigned privacy roles and responsibilities received role-based training before being authorized to access Federal information or information systems or performing assigned duties during the reporting period? [60]

0%

11e Did the agency ensure that measures were in place to test the knowledge level of information system users in conjunction with privacy training? [61]

Yes

11f To what extent did the agency ensure that all personnel were held accountable for complying with agency-wide privacy requirements and policies? [62] (Select one of the following.)

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

11g Did the agency have 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? [63]

Yes

11h Did the agency ensure that Federal employees had read and agreed to abide by the rules of behavior referenced in question 11g prior to being granted access? [64]

Yes

[57]See id. app. I § 4(h)(1).
[58]See id.
[59]See id. app. I § 4(h)(5).
[60]See id.
[61]See id. app. I § 4(h)(4).
[62]See id. app. I § 3(b)(9).
[63]See id. app. I § 4(h)(6).
[64]See id. app. I § 4(h)(7).

Section 12: Incident Response

12a For which of the following actions did the agency include policies and procedures in the agency`s breach response plan? [65] (Select all that apply.)

- 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? [66]

Yes

12c Did the agency have a breach response team composed of agency officials designated by the head of the agency that could be convened to lead the agency`s response to a breach? [67]

Yes

12d Did the agency`s breach response team referenced in question 12c participate in at least one tabletop exercise during the reporting period? [68]

Yes

12e How many breaches, as OMB M-17-12 defines the term breach, were reported within the agency during the reporting period? [69]

0

12f How many breaches, as OMB M-17-12 defines the term breach, did the agency report to the DHS Cybersecurity and Infrastructure Security Agency (CISA) during the reporting period? [70]

0

[65]See OMB M-17-12, Preparing for and Responding to a Breach of PersonallyIdentifiable Information, §§ VII, XI (Jan. 3, 2017).
[66] See id. §§ X.B, XI.
[67]See id. §§ VII.A, XI.
[68]See id. §§ X.A, XI.
[69]See id. §§ III.C, XI. As stated in OMB M-17-12, “[e]ach agencyshall require all individuals with access to the agency’s Federal informationand information systems to report a suspected or confirmed breach to the agencyas soon as possible and without unreasonable delay.” Id. § VI.
[70]See id. at §§ VII.D.1, XI.

Section 13: Risk Management Framework

13a Which of the following activities were guided and informed by the agency`s implementation of a risk management framework? [71] (Select all that apply.)

- 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 Did the agency designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls? [72]

Yes

13c Did the agency maintain a written privacy continuous monitoring strategy? [73]

Yes

13d Did the agency maintain an agency-wide privacy continuous monitoring program? [74]

Yes

[71]See OMB Circular No. A-130, app. I § 3(a), (b)(5).
[72]See id. app. I § 4(e)(5); see also id. § 10(a)(14),(26), (66), (86).
[73] The SAOP shall develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk managementtiers and ensures that the privacy controls are effectively monitored on anongoing basis by assigning an agency-defined assessment frequency to eachcontrol that is sufficient to ensure compliance with applicable privacyrequirements and to manage privacy risks. See id. app. I § 4(d)(9),(e)(2).
[74] The SAOP shall establish and maintain an agency-wideprivacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that maypose privacy risks; monitors changes to information systems and environments ofoperation that create, collect, use, process, store, maintain, disseminate,disclose, or dispose of PII; and conducts privacy control assessments to verifythe continued effectiveness of all privacy controls selected and implemented atthe agency across the agency risk management tiers to ensure continued compliancewith applicable privacy requirements and manage privacy risks. See id.app. I § 4(d)(10)-(11), (e)(2).

Section 14: Privacy Program Website

14a Did the agency have a Privacy Program Page located at (or redirected from) www.[agency].gov/privacy? [75]

Yes

14b Did the agency`s Privacy Program Page include a list and provide links to complete, up-to-date versions [76] of all agency`sORNs? [77]

Yes

14c Did the agency`s Privacy Program Page include a list and provide links to all PIAs? [78]

Yes

14d Did 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? [79]

Yes

14e Did 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? [80]

No

14e.1 Explanation

The page does not include citations or link to final Federal Regiser exemptions rules. This content will be added as appropriate during scheduled page updates.

14f Did 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)? [81]

Yes

14g Did 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? [82]

Yes

14h Did the agency`s Privacy Program Page include a list and provide links to all publicly available agency reports on privacy? [83]

Yes

14i Did 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)? [84]

Yes

14j Did the agency`s Privacy Program Page include appropriate agency contact information for individuals who wish to submit a privacy-related question or complaint? [85]

Yes

14k Did the agency`s Privacy Program Page identify the agency`s SAOP and include appropriate contact information for the SAOP s office?

No

14k.1 Explanation

The agency Privacy Office is revising the Privacy Program page to identify the SAOP and contact information. The website has contact infornation for the Privacy Office.

[75]See OMB M-23-22, Delivering a Digital-First Public Experience § III(A)(9)(a)(Sept. 22, 2023); see also OMB Circular No. A-108, § 15.
[76]This requires agencies to provide the following: (1) A list of all of theagency's systems of records; (2) Citations and links to all Federal Registernotices that comprise the SORN for each system of records; and (3) For anySORNs that are comprised of multiple Federal Register notices, anunofficial consolidated version of the SORN that describes the current systemof records and allows members of the public to view the SORN in its entirety ina single location. OMB Circular No. A-108, § 15(a).
[77]See OMB M-23-22, § III(A)(9)(a); seealso OMB Circular No. A-108, § 15(a).
[78]See OMB M-23-22, § III(A)(9)(a).
[79]See id.; see also OMB Circular No. A-108, § 15(b).
[80] See OMBM-23-22, § III(A)(9)(a); see also OMB Circular No. A-108, § 15(c).
[81]See OMB M-23-22, § III(A)(9)(a); see also OMB Circular No. A-108,§ 15(d).
[82]See OMB M-23-22, § III(A)(9)(a).
[83]See id.
[84]See id.; see also OMB Circular No. A-108, § 15(e).
[85] See OMBM-23-22, § III(A)(9)(a).
[86]See id.