Fiscal Year 2025
Senior Agency Official for Privacy
Federal Information Security Modernization Act of 2014
Reporting Metrics

August 2025

Contents

FY 2025 SAOP FISMA Metrics

OMB collects the annual Senior Agency Official for Privacy (SAOP) FISMA Metrics pursuant to the authority in the Federal Information Security Modernization Act of 2014,[1] the Privacy Act of 1974,[2] the Paperwork Reduction Act of 1995,[3] the E-Government Act of 2002,[4] Executive Order 13719,[5] OMB Circular No. A-130,[6] OMB Circular No. A-108,[7] and other laws, regulations, and policies.

Each year, OMB issues guidance instructing each SAOP to review the administration of the agency's privacy program and report compliance data to OMB. The following questions facilitate that review for the FISMA reporting period covering October 1, 2024, through September 30, 2025. Before submitting the responses to the following questions, please ensure that explanations are provided where requested in the accompanying text boxes.

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?[8]

- Yes – for the duration of the reporting period, the agency had an SAOP designated by the head of the agency
- No – during the reporting period, there was a period in which there was no SAOP designated by the head of the agency (if selected, please explain in the text box, including the amount of time without such an SAOP)

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?[9]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – there was no SAOP designated by the head of the agency

1c. The SAOP is required to have the necessary position, expertise, and authority to serve in the role.[10] Which of the following requirements were met? (Select all that apply.)

---

[1] 44 U.S.C. Chapter 35.
[2] 5 U.S.C. § 552a.
[3] 44 U.S.C. Chapter 35 et seq.
[4] 44 U.S.C. § 3501 note.
[5] Exec. Order No. 13719, Establishment of the Federal Privacy Council, 81 Fed. Reg. 7687 (Feb. 12, 2016).
[6] OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).
[7] OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Dec. 2016).
[8] *See* Executive Order 13719, § 3; *see also* OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 15, 2016).
[9] *See* OMB M-16-24, at 4.
[10] The role and requirements for the SAOP are described in OMB guidance. *See generally* OMB M-16-24.

- ⎦ Position
- ⎦ Expertise
- ⎦ Authority
- ⎦ None of the above (if selected, please explain in the text box)
- ⎦ Not applicable – there was no SAOP designated by the head of the agency

1d. For which of the following areas did the SAOP have the necessary role and responsibilities within the agency?[11] (Select all that apply.)

- ⎦ Policy making
- ⎦ Compliance
- ⎦ Risk management
- ⎦ None of the above (if selected, please explain in the text box)
- ⎦ Not applicable – there was no SAOP designated by the head of the agency

1e. Did the agency maintain an up-to-date privacy program plan?[12]

- Yes
- No (if selected, please explain in the text box)

1f. For which of the following areas did the agency's privacy program plan include a description?[13] (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
- ⎦ None of the above (if selected, please explain in the text box)
- ⎦ Not applicable – the agency did not have a privacy program plan

2. Information Systems

2a. Did the agency maintain an inventory of the agency's information systems[14] that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable

[11] *See id*. at 3–4.

[12] Each agency is required to develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program. *See* OMB Circular No. A-130, app. I § 4(c)(2), (e)(1).

[13] *See id*. app. I § 4(c)(2).

[14] The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C. § 3502(8). The term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology. *Id.* § 3502(6). The term "Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. OMB Circular No. A-130, § 10(a)(23).

information (PII)?[15]

- Yes
- No (if selected, please explain in the text box)

2b. What is the number of information systems reported in response to question 1.1 of the FY 2025 Chief Information Officer FISMA Metrics that were used during the reporting period to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

2c. What is the number of information systems reported in question 2b that the agency authorized or reauthorized to operate during the reporting period?[16]

2d. What is the 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?[17]

2e. What is the 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?[18]

2f. What is the 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?[19]

2g. What is the 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?[20]

3. Information Technology Systems and Privacy Impact Assessments

3a. Did the agency maintain an inventory of the agency's information technology[21] (IT) systems

[15] *See* OMB Circular No. A-130, § 5(a)(1)(a)(ii). The term "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. *Id.* § 10(a)(57).

[16] "Authorization to operate" is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. *Id.* app. I § 4(d).

[17] *See id.* app. I § 4(a)(2), (e)(7).

[18] Agencies shall develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls. *See id*. app. I § 4(c)(9), (e)(8).

[19] *See id.* app. I § 4(e)(3).

[20] *See id.* app. I § 4(e)(9).

[21] The term "information technology" means any services or equipment, or interconnected system(s) or subsystem(s) of

that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

- Yes
- No (if selected, please explain in the text box)

3b. What is the 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 was required to conduct a privacy impact assessment (PIA) under the E-Government Act of 2002?

3c. What is the number of IT systems reported in question 3b that were covered by an up-to-date PIA?[22]

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]
- ⌋ None of the above (if selected, please explain in the text box)
- ⌋ Not applicable – the agency did not have a written policy for PIAs

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[26]
- ⌋ Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated[27]
- ⌋ Ensuring that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks[28]
- ⌋ None of the above (if selected, please explain in the text box)

---

equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. *See id.* § 10(a)(45).

[22] 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).

[23] *See id*.

[24] *See id*.

[25] *See id*.

[26] *See id*.

[27] *See id*.

[28] *See id*.

4. Systems of Records

4a. What is the number of Privacy Act systems of records[29] maintained by the agency during the reporting period (including those operated by a service provider or a contractor on behalf of the agency)?

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*?[30]

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?[31]

- Yes
- No (if selected, please explain in the text box)

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]
- ⌋ None of the above (if selected, please explain in the text box)

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

[29] The term "system of records" means a group of any records under the control of any agency 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. 5 U.S.C. § 552a(5).
[30] Agencies are required to publish a SORN in the *Federal Register* when establishing a new system of records and must also publish notice in the *Federal Register* when making significant changes to an existing system of records. For the purposes of this question, an up-to-date SORN is a published SORN that reflects any significant changes that have been made to the system of records. OMB Circular No. A-108, § 6(a).
[31] *See* 5 U.S.C. § 552a(e)(4).
[32] *See id.* § 552a(e)(3).
[33] *See id.* § 552a(d).
[34] *See id.* § 552a(e)(1); OMB Circular No. A-108, § 12(a).
[35] *See* 5 U.S.C. § 552a(e)(4); OMB Circular No. A-108, § 12(b).
[36] *See* OMB Circular No. A-108, § 12(b).
[37] *See id.*
[38] *See* 5 U.S.C. § 552a(r); OMB Circular No. A-108, § 12(b).

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]
- ⎦ None of the above (if selected, please explain in the text box)
- ⎦ Not applicable – the agency did not maintain any Privacy Act systems of records during the reporting period

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?[43] (Select one of the following.)

- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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?[44] (Select one of the following.)

- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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

[39] *See* OMB Circular No. A-108, § 12(c).
[40] *See id.* § 12(d).
[41] *See id.* § 12(e).
[42] *See id.* § 12(f).
[43] *See* OMB Circular No. A-130, § 5(f)(1)(e).
[44] *See id.* § 5(f)(1)(d).

6. Social Security Numbers

6a. Did the agency have an inventory of the agency's collection, maintenance, and use of Social Security numbers (SSNs)?[45]

- Yes
- No
- Not applicable – the agency has not collected, maintained, or used SSNs

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
- No
- Not applicable – the agency has not done one or more of the following: (1) collected, maintained, or used SSNs; (2) maintained the inventory of its collection, maintenance, and use of SSNs referenced in question 6a; or (3) maintained the inventory of information systems referenced in question 2a

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
- No

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
- No
- Not applicable – the agency did not have the written policy referenced in question 6c

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
- No
- Not applicable – the agency did not have the written policy referenced in question 6c

6f. Did the agency take steps to eliminate the unnecessary collection, maintenance, and use of SSNs?[46]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – (1) the agency did not collect, maintain, or use SSNs during the reporting period, and/or (2) the agency had already eliminated all unnecessary collection, maintenance, and use of SSNs by the agency before the reporting period

[45] Agencies are not required to have an inventory of collection, maintenance, and use of SSNs. However, agencies need to have a sufficient evidentiary basis to determine whether they have met the requirement to eliminate unnecessary collection, maintenance, and use of SSNs. *See id.* § 5(f)(1)(f).

[46] Agencies are required to take steps to eliminate unnecessary collection, maintenance, and use of SSNs, and explore alternatives to the use of SSNs as a personal identifier. *Id.*

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
- ⎦ The agency's public applications (*e.g.*, mobile applications, web applications)
- ⎦ The agency's public social media accounts
- ⎦ Other public-facing digital services used by the agency
- ⎦ None of the above (if selected, please explain in the text box)

7b. In accordance with the E-Government Act of 2002 and OMB guidance,[47] for which of the following digital services did the agency maintain and post privacy policies? (Select all that apply.)

- ⎦ The agency's public websites
- ⎦ The agency's public applications (*e.g.*, mobile applications, web applications)
- ⎦ The agency's public social media pages and profiles
- ⎦ Other public-facing digital services used by the agency
- ⎦ None of the above (if selected, please explain in the text box)

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
- ⎦ The agency's public applications (*e.g.*, mobile applications, web applications)
- ⎦ Other public-facing digital services used by the agency
- ⎦ None of the above (if selected, please explain in the text box)

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

- Yes
- No
- Not applicable – the agency did not use social media

7e. Did the agency use web measurement and customization technologies on any website or mobile application?[48]

- Yes
- No

7f. Did the agency review the use of web measurement and customization technologies to ensure compliance with all laws, regulations, and OMB guidance?[49]

- Yes
- No (if selected, please explain in the text box)

[47] *See id.* § 5(f)(1)(j).
[48] *See* OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010).
[49] *See id.*

- Not applicable – the agency did not use web measurement and customization technologies on any website or mobile application

8. Budget and Acquisition

8a. Did the agency identify and plan for the resources needed to implement the agency's privacy program?[50]
- Yes
- No (if selected, please explain in the text box)

8b. Did the agency have a policy that includes explicit criteria for analyzing privacy risks when considering IT investments?[51]
- Yes
- No (if selected, please explain in the text box)

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?[52]
- Yes
- No (if selected, please explain in the text box)

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?[53] (Select one of the following.)
- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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?[54]
- Yes
- No (if selected, please explain in the text box)

8f. What is the number of information systems and components used during the reporting period

[50] *See* OMB Circular No. A-130, app. I § 4(b)(1).
[51] *See id.* § 5(d)(3).
[52] *See id.* § 5(a)(3)(e)(ii).
[53] *See id.* app. I § 4(b)(3).
[54] *See id.* app. I § 3(b)(10).

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?

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?[55] (Select one of the following.)

- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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?[56] (Select one of the following.)

- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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?[57] (Select one of the following.)

- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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

[55] *See id.* § 5(a)(1)(b)(ii); *id.* app. I § 4(j)(1).
[56] *See id.* app. I § 4(j)(3).
[57] *See id.* app. I § 4(j)(2)(a).

9d. Did the agency maintain a mandatory agency-wide privacy awareness and training program for all contractors?[58]

- Yes
- No (if selected, please explain in the text box)

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?[59]

- Yes
- No (if selected, please explain in the text box)

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?[60]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not have such rules of behavior

10. <u>Privacy Workforce Management</u>

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

- Yes
- No (if selected, please explain in the text box)

10b. Did the agency assess its hiring, training, and professional development needs with respect to privacy?[61]

- Yes
- No (if selected, please explain in the text box)

10c. Did the agency have a workforce planning process to ensure that it accounts for privacy workforce needs?[62]

- Yes
- No (if selected, please explain in the text box)

10d. Did the agency have a set of competency requirements for privacy staff, including program managers and privacy leadership positions?[63]

- Yes
- No (if selected, please explain in the text box)

[58] *See id.* app. I § 4(h)(1), (4)–(5).
[59] *See id.* app. I § 4(h)(6).
[60] *See id.* app. I § 4(h)(7).
[61] *See id.* § 5(c)(6).
[62] *See id.* § 5(c)(1).
[63] *See id.*

11. Training and Accountability

11a. Did the agency maintain a mandatory agency-wide privacy awareness and training program for all Federal employees?[64]

- Yes
- No (if selected, please explain in the text box)

11b. What percentage of Federal employees participated in a mandatory agency-wide privacy awareness and training program during the reporting period?[65]

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?[66]

- Yes
- No (if selected, please explain in the text box)

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?[67]

11e. Did the agency ensure that measures were in place to test the knowledge level of information system users in conjunction with privacy training?[68]

- Yes
- No (if selected, please explain in the text box)

11f. To what extent did the agency ensure that all personnel were held accountable for complying with agency-wide privacy requirements and policies?[69] (Select one of the following.)

- Processes did not exist (if selected, please explain in the text box)
- Processes existed; however, they were not fully documented and/or did not cover all relevant aspects
- Processes were fully documented and implemented and covered all relevant aspects
- 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?[70]

---

[64] *See id*. app. I § 4(h)(1).
[65] *See id.*
[66] *See id.* app. I § 4(h)(5).
[67] *See id.*
[68] *See id.* app. I § 4(h)(4).
[69] *See id.* app. I § 3(b)(9).
[70] *See id.* app. I § 4(h)(6).

- Yes
- No (if selected, please explain in the text box)

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?[71]
- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not have such rules of behavior

12. Breach Response

12a. For which of the following actions did the agency include policies and procedures in the agency's breach response plan?[72] (Select all that apply.)
- ⎦ Reporting a breach
- ⎦ Investigating a breach
- ⎦ Managing a breach
- ⎦ None of the above (if selected, please explain in the text box)
- ⎦ Not applicable – the agency did not have a breach response plan (if selected, please explain in the text box)

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?[73]
- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not have a breach response plan

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?[74]
- Yes
- No (if selected, please explain in the text box)

12d. Did the agency's breach response team referenced in question 12c participate in at least one tabletop exercise during the reporting period?[75]
- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not have such a breach response team

12e. How many breaches, as OMB M-17-12 defines the term "breach," were reported within the

[71] *See id.* app. I § 4(h)(7).
[72] *See* OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, §§ VII, XI (Jan. 3, 2017).
[73] *See id.* §§ X.B, XI.
[74] *See id.* §§ VII.A, XI.
[75] *See id.* §§ X.A, XI.

agency during the reporting period?[76]

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?[77]

13. <u>Risk Management Framework</u>

13a. Which of the following activities were guided and informed by the agency's implementation of a risk management framework?[78] (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
- ⎦ None of the above (if selected, please explain in the text box)
- ⎦ Not applicable – the agency did not implement a risk management framework (if selected, please explain in the text box)

13b. Did the agency designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls?[79]

- Yes
- No (if selected, please explain in the text box)

13c. Did the agency maintain a written privacy continuous monitoring strategy?[80]

- Yes
- No (if selected, please explain in the text box)

13d. Did the agency maintain an agency-wide privacy continuous monitoring program?[81]

- Yes
- No (if selected, please explain in the text box)

---

[76] *See id.* §§ III.C, XI. As stated in OMB M-17-12, "[e]ach agency shall require all individuals with access to the agency's Federal information and information systems to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay." *Id.* § VI.

[77] *See id.* at §§ VII.D.1, XI.

[78] *See* OMB Circular No. A-130, app. I § 3(a), (b)(5).

[79] *See id.* app. I § 4(e)(5); *see also id.* § 10(a)(14), (26), (66), (86).

[80] 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 management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. *See id.* app. I § 4(d)(9), (e)(2).

[81] The SAOP shall establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. *See id.* app. I § 4(d)(10)–(11), (e)(2).

14. <u>Privacy Program Website</u>

14a. Did the agency have a Privacy Program Page located at (or redirected from) www.[agency].gov/privacy?[82]

- Yes
- No (if selected, please explain in the text box)

14b. Did the agency's Privacy Program Page include a list and provide links to complete, up-to-date versions[83] of all agency SORNs?[84]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not maintain any Privacy Act systems of records

14c. Did the agency's Privacy Program Page include a list and provide links to all PIAs?[85]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not maintain, operate, or use any IT systems that required a PIA

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?[86]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not participate in any matching programs

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?[87]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not claim any Privacy Act exemptions for their systems of records

14f. Did the agency's Privacy Program Page include a list and provide links to all Privacy Act

[82] *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.

[83] This requires agencies to provide the following: (1) A list of all of the agency's systems of records; (2) Citations and links to all *Federal Register* notices that comprise the SORN for each system of records; and (3) For any SORNs that are comprised of multiple *Federal Register* notices, an unofficial consolidated version of the SORN that describes the current system of records and allows members of the public to view the SORN in its entirety in a single location. OMB Circular No. A-108, § 15(a).

[84] *See* OMB M-23-22, § III(A)(9)(a); *see also* OMB Circular No. A-108, § 15(a).

[85] *See* OMB M-23-22, § III(A)(9)(a).

[86] *See id.*; *see also* OMB Circular No. A-108, § 15(b).

[87] *See* OMB M-23-22, § III(A)(9)(a); *see also* OMB Circular No. A-108, § 15(c).

implementation rules promulgated pursuant to 5 U.S.C. § 552a(f)?[88]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not maintain any Privacy Act systems of records

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?[89]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not have any publicly available agency policies on privacy

14h. Did the agency's Privacy Program Page include a list and provide links to all publicly available agency reports on privacy?[90]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not have any publicly available agency reports on privacy

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)?[91]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – the agency did not maintain any Privacy Act systems of records

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?[92]

- Yes
- No (if selected, please explain in the text box)

14k. Did the agency's Privacy Program Page identify the agency's SAOP and include appropriate contact information for the SAOP's office?[93]

- Yes
- No (if selected, please explain in the text box)
- Not applicable – there was no SAOP designated by the head of the agency

[88] *See* OMB M-23-22, § III(A)(9)(a); *see also* OMB Circular No. A-108, § 15(d).
[89] *See* OMB M-23-22, § III(A)(9)(a).
[90] *See id.*
[91] *See id.*; *see also* OMB Circular No. A-108, § 15(e).
[92] *See* OMB M-23-22, § III(A)(9)(a).
[93] *See id.*