Fiscal Year 2023
Senior Agency Official for Privacy
Federal Information Security Modernization Act of 2014
Reporting Metrics
v1.0

August 2023

Document History

Version	Date	Comments	See/Page
1.0	August 2023	FY 2023 SAOP FISMA Metrics	All

Contents

FY 2023 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 A-130,[6] OMB Circular 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.

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?[8]

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?[9] (Indicate "N/A" if the head of the agency has not designated an SAOP. Only indicate "N/A" if the answer to question 1a is "No.")

1c. Does the SAOP have the necessary position, expertise, and authority to serve in the role of SAOP?[10] (Select all that apply or indicate "N/A" if the head of the agency has not designated an SAOP. Only indicate "N/A" if the answer to question 1a is "No.")

- ⎦ Position
- ⎦ Expertise
- ⎦ Authority

1d. Does the SAOP have the necessary role and responsibilities within the agency for each of the following?[11] (Select all that apply or indicate "N/A" if the head of the agency has not designated an SAOP. Only indicate "N/A" if the answer to question 1a is "No.")

- ⎦ Policy making
- ⎦ Compliance
- ⎦ Risk management activities

1e. Has the agency developed and maintained a privacy program plan?[12]

---

[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. 7685 (Feb. 12, 2016).
[6] OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).
[7] OMB Circular 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* OMB M-16-24.
[11] *See id*. at 3–4.
[12] Agencies are 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

1f. Does the agency's privacy program plan include a description of each of the following?[13] (Select all that apply or indicate "N/A" if the agency has not developed and maintained a privacy program plan. Only indicate "N/A" if the answer to question 1e is "No.")

- ⎦ 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

2. Information Systems

2a. Does 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 information (PII)?[15]

2b. Number of information systems reported in response to question 1.1 of the FY 2022 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.[16]

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.[17]

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.[18]

---

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 A-130, app. I § 4(c)(2), 4(e)(1).

[13] *See id.* at 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 A-130, § 10(a)(23).

[15] *See id.* § 5(a)(1)(a)(ii), 5(f)(1)(e). 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. OMB Circular A-130, § 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. OMB Circular A-130, app. I § 4(d).

[17] *See id.* app. I § 4(a)(2), 4(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

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.[19]

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.[20]

3. Information Technology Systems and Privacy Impact Assessments

3a. Does the agency maintain an inventory of the agency's information technology[21] (IT) systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?

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.[22]

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 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]

---

controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls. *See* OMB Circular A-130, app. I § 4(c)(9), (e)(8).

[19] *See id.* app. I § 4(e)(3).

[20] *See* OMB Circular A-130, app. I § 4(e)(9).

[21] The term "information technology" means any services or equipment, or interconnected system(s) or subsystem(s) of 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* OMB Circular A-130, Managing Information as a Strategic Resource, § 10(a)(45) (Sept. 26, 2003).

[22] Agencies are 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.* at Appendix II § 5(e) (July 28, 2016).

[23] *See id*.

[24] *See id*.

[25] *See id*.

3e. Does the agency have a process or procedure for each of the following? (Select all that apply. If the agency does not have such a process or procedure, leave it blank.)

- ⌋ 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]

4. Systems of Records

4a. 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. 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*.[30]

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?[31]

4d. Does the agency have a process for each of the following? (Select all that apply. If the agency does not have such a process, leave it blank.)

- ⌋ 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. 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 did not maintain any Privacy Act systems of records during the reporting period. Only indicate "N/A" if the answer to question 4a is "Zero.")

- ⌋ 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]

---

[26] *See id*.
[27] *See id*.
[28] *See id*.
[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 A-108, § 6(a).
[31] *See* 5 U.S.C. § 552a(e)(4).
[32] *See id.* at § 552a(e)(3).
[33] *See id.* at § 552a(d).
[34] *See* 5 U.S.C. § 552a(e)(1); OMB Circular A-108, § 12(a).
[35] *See* 5 U.S.C. § 552a(e)(4); OMB Circular A-108, § 12(b).

- ⎦ SORNs are published in the *Federal Register*[36]
- ⎦ SORNs include the information, and are drafted in the format, required by OMB Circular 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]

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

- ⎦ Processes do not exist
- ⎦ Processes exist; however, they are not fully documented and/or do not cover all relevant aspects
- ⎦ Processes are fully documented and implemented and cover all relevant aspects
- ⎦ 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?[44] (Select one of the following.)

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

[36] *See* OMB Circular A-108, § 12(b).
[37] *See id.*
[38] *See* 5 U.S.C. § 552a(r); OMB Circular A-108, § 12(b).
[39] *See* OMB Circular A-108, at § 12(c).
[40] *See id.* at § 12(d).
[41] *See id.* at § 12(e).
[42] *See id.* at § 12(f).
[43] *See* OMB Circular A-130, § 5(f)(1)(e).
[44] *See id* at § 5(f)(1)(d).

reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current

6. Social Security Numbers

6a. Does the agency have an inventory of the agency's collection and use of Social Security numbers (SSNs)?[45] (Indicate "N/A" if the agency does not collect, maintain, or use SSNs.)

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 as described in question 2a. Only indicate "N/A" if the answer to question 6a is "N/A" or "No," and/or if the answer to question 2a is "No.")

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

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 as described in question 6c. Only indicate "N/A" if the answer to question 6c is "No.")

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 as described in question 6c. Only indicate "N/A" if the answer to question 6c is "No.")

6f. Has the agency taken steps during the reporting period to eliminate the unnecessary collection, maintenance, and use of SSNs?[46] (Indicate "N/A" if the agency does not collect, maintain, or use SSNs. If indicating "N/A" because the agency does not collect, maintain, or use SSNs, ensure that the answer to question 6a also is "N/A." Also indicate "N/A" if the agency does collect, maintain, or use SSNs but had already eliminated all unnecessary collection, maintenance, and use of SSNs by the agency before the reporting period.)

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 maintain an inventory of any digital services.)

- ⌋ 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

[45] Agencies are not required to have an inventory of collection 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 and use of SSNs. *See* OMB Circular A-130, § 5(f)(1)(f).

[46] Agencies are required to take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier. OMB Circular A-130, § 5(f)(1)(f).

7b. In accordance with the E-Government Act of 2002 and OMB guidance,[47] 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.)

- ⎦ 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

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 maintain any of the following.)

- ⎦ 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

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.)

7e. During the reporting period, did the agency use web management and customization technologies on any website or mobile application?[48]

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?[49] (Indicate "N/A" if the agency does not use web management and customization technologies on any website or mobile applications. Only indicate "N/A" if the answer to question 7e is "No.")

8. Budget and Acquisition

8a. Does the agency identify and plan for the resources needed to implement the agency's privacy program?[50]

8b. Does the agency have a policy that includes explicit criteria for analyzing privacy risks when considering IT investments?[51]

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?[52]

[47] *See* OMB Circular A-130, § 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.*
[50] *See* OMB Circular A-130, app. I § 4(b)(1).
[51] *See id.* § 5(d)(3).
[52] *See id.* § 5(a)(3)(e)(ii).

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

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

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?[54]

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 agency does not 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. Only indicate "N/A" if the answer to question 8e is "No.")

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

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

[53] *See id.* app. I § 4(b)(3).
[54] *See id.* app. I § 3(b)(10).
[55] *See id.* § 5(a)(1)(b)(ii); *id.* app. I § 4(j)(1).

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

- ⎦ Processes do not exist
- ⎦ Processes exist; however, they are not fully documented and/or do not cover all relevant aspects
- ⎦ Processes are fully documented and implemented and cover all relevant aspects
- ⎦ 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?[57] (Select one of the following.)

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

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

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?[59]

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?[60] (Indicate "N/A" if the agency does not have established rules of behavior as described in question 9e. Only indicate "N/A" if the answer to question 9e is "No.")

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

10a. Does the agency ensure that the agency's privacy workforce has the appropriate knowledge and skill?[61]

[56] *See id.* app. I § 4(j)(3).
[57] *See id.* app. I § 4(j)(2)(a).
[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)(2).

10b. Has the agency assessed its hiring, training, and professional development needs with respect to privacy during the reporting period?[62]

10c. Has the agency developed a workforce planning process to ensure that it accounts for privacy workforce needs?[63]

10d. Has the agency developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions?[64]

11. <u>Training and Accountability</u>

11a. Does the agency provide foundational privacy training to its Federal employees (including managers and senior executives)?[65]

11b. What percentage of the agency's Federal employees (including managers and senior executives) received foundational privacy training during the reporting period?[66] (Indicate "N/A" if the agency does not provide foundational privacy training as described in question 11a. Only indicate "N/A" if the answer to question 11a is "No.")

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?[67]

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 as described in question 11c. Only indicate "N/A" if the answer to question 11c is "No.")

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

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

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

---

[62] *See id.* § 5(c)(6).
[63] *See id.* § 5(c)(1).
[64] *See id.*
[65] *See id*. app. I § 4(h)(4); *see also id.* app. I § 4(h)(1).
[66] *See id.*
[67] *See id.* app. I § 4(h)(5); *see also id.* app. I § 4(h)(1).
[68] *See id.* app. I § 4(h)(4).
[69] *See id.* app. I § 3(b)(9).

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?[70]

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?[71] (Indicate "N/A" if the agency does not have established rules of behavior as described in question 11g. Only indicate "N/A" if the answer to question 11g is "No.")

12. <u>Breach Response</u>

12a. Does the agency have a breach response plan[72] 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?[73] (Indicate "N/A" if the agency does not have a breach response plan.)

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?[74]

12d. Did the agency's breach response team participate in at least one tabletop exercise during the reporting period?[75] (Indicate "N/A" if the agency does not have a breach response team as described in question 12c. Only indicate "N/A" if the answer to question 12c is "No.")

12e. How many breaches, as OMB Memorandum M-17-12 defines the term "breach," were reported within the agency during the reporting period?[76]

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?[77]

---

[70] *See id.* app. I § 4(h)(6).
[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.
[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.

13. Risk Management Framework

13a. Has the agency implemented a risk management framework to guide and inform each of the following?[78] (Select all that apply or indicate "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?[79]

13c. Has the agency developed and maintained a written privacy continuous monitoring strategy?[80]

13d. Has the agency established and maintained an agency-wide privacy continuous monitoring program?[81]

14. Privacy Program Website

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

14b. Does the agency's Privacy Program Page include a list and provide links to complete, up-to-date versions of all agency SORNs?[83] (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records. Only indicate "N/A" if the answer to question 4a is "Zero.")

14c. Does the agency's Privacy Program Page include a list and provide links to all PIAs?[84] (Indicate "N/A" if the agency does not maintain, operate, or use any IT systems that require a PIA. Only indicate "N/A" if the answer to question 3b is "Zero.")

---

[78] *See* OMB Circular 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).
[82] *See* OMB M-17-06, § 6(A).
[83] *See id.* § 6(A)(1)(a).
[84] *See id.* § 6(A)(1)(b).

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?[85] (Indicate "N/A" if the agency does not participate in any matching programs.)

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?[86] (Indicate "N/A" if the agency has not claimed any Privacy Act exemptions for their systems of records.)

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)?[87] (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records. Only indicate "N/A" if the answer to question 4a is "No.")

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?[88] (Indicate "N/A" if the agency does not have any publicly available agency policies on privacy.)

14h. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency reports on privacy?[89] (Indicate "N/A" if the agency does not have any publicly available agency reports on privacy. If indicating "N/A," ensure the answer to question 14g also is "N/A.")

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)?[90] (Indicate "N/A" if the agency does not maintain any Privacy Act systems of records. Only indicate "N/A" if the answer to question 4a is "No.")

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?[91]

14k. Does the agency's Privacy Program Page identify the agency's SAOP and include appropriate contact information for the SAOP's office?[92] (Indicate "N/A" if the head of the agency has not designated an SAOP. Only indicate "N/A" if the answer to question 1a is "No.")

[85] *See id.* § 6(A)(1)(c).
[86] *See id.* § 6(A)(1)(d).
[87] *See id.* § 6(A)(1)(e).
[88] *See id.* § 6(A)(1)(f).
[89] *See id.* § 6(A)(1)(g).
[90] *See id.* § 6(A)(1)(h).
[91] *See id.* § 6(A)(1)(i).
[92] *See id.* § 6(A)(1)(j).