FY 2016

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

Prepared by:

US Department of Homeland Security
Office of Cybersecurity and Communications
Federal Network Resilience

June 29, 2016

Document History

Version	Date	Comments	See/Page
1.0	29 June 2016	Final FY16 SAOP FISMA Metrics	All

Contents

1 Information Systems

1a. Number of Federal information systems[1] reported in question 1.1 of the FY 2016 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).[2]

1b. Number of Federal information systems reported in question 1a that were approved by the SAOP prior to authorization or reauthorization.[3]

1c. Number of information technology[4] systems maintained or used by the agency (or by another entity on behalf of the agency) for which a privacy impact assessment (PIA) is required under the E-Government Act.

1d. Number of information technology systems reported in question 1c that are covered by an up-to-date PIA.[5]

1e. Number of Privacy Act systems of records[6] maintained by the agency (or by another entity on behalf of the agency).

1f. Number of Privacy Act systems of records reported in question 1e for which an up-to-date system of records notice (SORN) has been published in the *Federal Register*.[7]

2 Agency Privacy Program[8]

2a. Does the SAOP have the necessary skills, expertise, and knowledge of privacy-related matters to carry out the privacy-related functions required in law and OMB policies?

2b. In addition to the SAOP, does the agency have a career Senior Executive Service employee who has privacy expertise and reports to the SAOP?

2c. How many total staff (full-time equivalent) at the agency (not including staff at sub-agencies, components, and programs) work at least half the time on privacy-related functions?[9]

2d. How many total contractors at the agency (not including contractors at sub-agencies, components, and programs) work at least half the time on privacy-related functions?

2e. How many total staff (full-time equivalent) at sub-agencies, components, and programs work at least half the time on privacy-related functions?

2f. How many total contractors at sub-agencies, components, and programs work at least half the time on privacy-related functions?

2g. Is the agency up-to-date with its review of its PII holdings, pursuant to the requirements in OMB Memorandum M-07-16?[10]

2h. Can the agency demonstrate with documentation that the SAOP participates in agency privacy compliance and privacy risk management activities?

2i. Can the agency demonstrate with documentation that the SAOP participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals, as well as testimony and comments under OMB Circular A-19?

3 Privacy Program Website

3a. Provide the URL of the agency's central privacy program page (indicate "N/A" if not applicable).

3b. Provide the URL of the centrally located page on the agency website that provides

working links to the agency's PIAs (indicate "N/A" if not applicable).

3c. Provide the URL of the centrally located page on the agency's website that provides working links to the agency's published SORNs (indicate "N/A" if not applicable).

3d. Provide the URL of the centrally located page on the agency's website that provides an inventory of third-party websites, applications, and digital services used by the agency (indicate "N/A" if not applicable).

4 Privacy Act Processes

4a. Has the agency developed and implemented a written policy or process for determining whether a SORN is required when the agency collects or maintains information?[11]

4b. Has the agency developed and implemented a written policy or process for ensuring that a SORN is published in the *Federal Register* prior to the agency establishing or altering a system of records?

4c. Has the agency developed and implemented a written policy or process for determining whether changes to a system of records require the agency to publish a new or revised SORN in the *Federal Register*?

4d. Has the agency developed and implemented a written policy or process for ensuring that information collections include a Privacy Act Statement, if required?[12]

4e. Has the agency developed and implemented a written policy or process for receiving and processing individuals' requests for access and amendment to records?[13]

5 Privacy Impact Assessment Processes

5a. Has the agency developed and implemented a written policy or process for determining whether a PIA is required when the agency develops, procures, or uses an information technology system?[14]

5b. Has the agency developed and implemented a written policy or process to ensure that a PIA is conducted and approved before an information technology system that requires a PIA is developed, procured, or used?

5c. Has the agency developed and implemented a written policy or process for ensuring that systems owners, privacy officials, and information technology experts participate in conducting the PIA?

5d. Has the agency developed and implemented a written policy or process for making PIAs available to the public as required by law and OMB policy?

5e. Has the agency developed and implemented a written policy or process for monitoring the agency's information technology systems and practices to determine when and how PIAs should be updated?

5f. Has the agency developed and implemented a written policy or process for ensuring that PIAs are updated whenever a change to an information technology system, a change in agency practices, or another factor alters the privacy risks?

5g. Has the agency developed and implemented a written policy or process for assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained?

6 Privacy Training and Accountability

6a. Has the agency developed and implemented a policy to ensure that all employees and contractors with access to information resources receive privacy training?

6b. Does the agency require role-based privacy training for employees and contractors who have particular responsibilities before authorizing access to information resources?

6c. Has the agency established rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to information resources?

6d. Has the agency developed and implemented a policy to ensure that employees and contractors are held accountable for complying with privacy requirements and managing privacy risks?

7 Websites, Mobile Applications, and Digital Privacy Practices

7a. Does the agency maintain an inventory of websites, applications, social media accounts, and other digital services provided or maintained by the agency?

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

7c. Does each of the agency's websites and mobile applications have a privacy policy?

7d. Has the agency developed and implemented a process to regularly review and update each of the agency's website and mobile application privacy policies?

7e. Does each of the agency's website and mobile application privacy policies clearly explain what information is collected and the purpose of the collection?

7f. Has the agency developed and implemented a process to address privacy in the development and use of mobile applications?

7g. Does the agency use web management and customization technologies on any website or mobile application?[15]

7h. Does the agency annually review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance (indicate "N/A" if the agency does not use web management and customization technologies)?

7i. Can the agency demonstrate, with documentation, the continued justification for, and approval to use, web management and customization technologies (indicate "N/A" if the agency does not use web management and customization technologies)?

7j. Number of requests for tier 3 web measurement and customization technologies approved by the SAOP during the reporting period.

8 Mandated Reviews

Did the agency perform the following reviews as described by OMB Circular No. A-130?[16] Indicate "N/A" if the review is not required.

8a. *Section (m) Contracts.* Review every two years a sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to

accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Privacy Act binding on the contractor and his or her employees.

8b. *Recordkeeping Practices.* Review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Privacy Act, paying particular attention to the maintenance of automated records.

8c. *Routine Use Disclosures.* Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.

8d. *Exemptions of Systems of Records.* Review every four years each system of records for which the agency has promulgated exemption rules pursuant to section (j) or (k) of the Privacy Act in order to determine whether such exemption is still needed.

8e. *Matching Programs.* Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Privacy Act, OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.

8f. *Privacy Act Training.* Review biennially agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Privacy Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.

8g. *Violations.* Review biennially the actions of agency personnel that have resulted either in the agency being found civilly liable under section (g) of the Privacy Act, or an employee being found criminally liable under the provisions of section (i) of the Privacy Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.

8h. *System of Records Notices.* Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed (e.g., the name of the system manager), ensure that an amended notice is published in the *Federal Register*.

9 Social Security Numbers

9a. Does the agency have a written inventory of the agency's collection and use of Social Security numbers (SSNs)?[17]

9b. Has the agency developed and implemented a written policy or procedure to ensure that any new collection or use of SSNs is necessary?[18]

9c. Has the agency developed and implemented a written policy or procedure to ensure that any necessary collection or use of SSNs remains necessary over time?

9d. Has the agency developed and implemented a written policy or procedure to ensure that any collection or use of SSNs associated with agency websites, online forms, mobile applications, and other digital services, are necessary and comply with applicable privacy and security requirements?

[1] The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *See* 44 U.S.C. § 3502.
[2] 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.
[3] Pursuant to OMB Memorandum M-14-04, Fiscal Year 2013 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management (Nov. 18, 2013), SAOP approval is required as a precondition for the issuance of an authorization to operate.
[4] The term "information technology" means any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.. *See* OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).
[5] Pursuant to OMB guidance, agencies are required to update PIAs as necessary. For example, an agency may be required to update a PIA to account for elements of the privacy analysis not identified during the initial stages of the information technology system life cycle; when a change to an information technology system creates new privacy risks; or to reflect changes to information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form. *See* OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).
[6] 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. *See* 5 U.S.C. 552a(5).
[7] Pursuant to the Privacy Act and OMB guidance, changes to a system of records may require the agency to publish a revised SORN in the *Federal Register*. *See* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975).
[8] For the purposes of the questions in section 2, an employee who works at least half the time on privacy-related functions is an employee who directly supports the agency's (or component's) privacy program by ensuring compliance with applicable privacy requirements, including drafting or reviewing privacy impact assessments, systems of records notices, or matching agreements; developing and evaluating privacy policies, including the agency's development and evaluation of legislative, regulatory, and other policy proposals that have privacy implications; and managing privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs or information systems. While there may be a number of functions that indirectly support the agency's (or component's) privacy program, such as Freedom of Information Act compliance and information security, agencies should not include those functions when determining whether an employee works at least half the time on privacy-related functions.
[9] Agencies may be asked to submit a list of the names of the staff persons reported in response to questions 2c, 2d, 2e, and 2f as an attachment to annual FISMA reports later this year.
[10] OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).
[11] *See* 5 U.S.C. § 552a(e)(4).
[12] *See id.* § 552a(e)(3).
[13] *See id.* § 552a(d).
[14] *See* OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).
[15] *See* OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010).
[16] *See* OMB Circular A-130, Management of Federal Information Resources (Nov. 28, 2000).
[17] Agencies are not required to have a written 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 and to provide annual progress reports to OMB.
[18] Agencies may be asked to submit these policies or procedures as an attachment to annual FISMA reports later this year.