FY 2015
Senior Agency Official for Privacy
Federal Information Security Management Act
Reporting Metrics
v1.0

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

14 January, 2015

Document History

Version	Date	Comments	Author	See/Page
1.0	01/14/2015	Initial Draft of FY15 SAOP FISMA Metrics	B. Frey J. McGrath A. Heydman C. Chase	All

Name:	FY 2015 Senior Agency Official for Privacy Federal Information Security Management Act Reporting Metrics
Created:	14 January, 2015
Authors:	Brian Frey, Jim McGrath, Amy Heydman, Craig Chase
Branch:	Cybersecurity Performance Management
Division:	Federal Network Resilience

1: Information Security Systems

1a. Number of Federal systems that contain personal information in an identifiable form

1b. Number of systems in 1a for which a Privacy Impact Assessment (PIA) is required under the E-Government Act

1c. Number of systems in 1b covered by a current PIA

1d. Number of systems in 1a for which a System of Records Notice (SORN) is required under the Privacy Act

1e. Number of systems in 1d for which a current SORN has been published in the Federal Register

2: PIAs and SORNs

2a. Provide the URL of the centrally located page on the organization web site that provides working links to organization PIAs (N/A if not applicable)

2b. Provide the URL of the centrally located page on the organization web site that provides working links to the published SORNs (N/A if not applicable)

3: Senior Agency Official for Privacy (SAOP) Responsibilities

3a. Can your organization demonstrate with documentation that the SAOP participates in all organization information privacy compliance activities?

3b. Can your organization 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?

3c. Can your organization demonstrate with documentation that the SAOP participates in assessing the impact of the organization's use of technology on privacy and the protection of personal information?

4: Privacy Training

4a. Does your organization have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations, and policies, and understand the ramifications of inappropriate access and disclosure?

4b. Does your organization have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) that handle personal information, that are directly involved in the administration of personal information or information technology systems, or that have significant information security responsibilities?

5: PIA and Web Privacy Policies and Processes

Does the organization have a written policy or process for each of the following?

5a. PIA Practices

5a(1). Determining whether a PIA is needed

5a(2). Conducting a PIA

5a(3). Evaluating changes in technology or business practices that are identified during the PIA process

5a(4). Ensuring systems owners, privacy officials, and IT experts participate in conducting the PIA

5a(5). Making PIAs available to the public as required by law and OMB policy

5a(6). Monitoring the organization's systems and practices to determine when and how PIAs should be updated

5a(7). Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained

5b. Web Privacy Practices

5b(1). Determining circumstances where the organization's web-based activities warrant additional consideration of privacy implications.

5b(2). Making appropriate updates and ensuring continued compliance with stated web privacy policies.

5b(3). Requiring machine-readability of public-facing organization web sites (i.e., use of P3P).

6: Conduct of Mandated Reviews

Did your organization perform the following reviews as required by the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007? Indicate "N/A" if not applicable.

6a. Section (m) Contracts

6b. Records Practices

6c. Routine Uses

6d. Exemptions

6e. Matching Programs

6f. Training

6g. Violations: Civil Action

6h. Violations: Remedial Action

6i. System of Records Notices

6j. (e) (3) Statements

6k. Privacy Impact Assessments and Updates

6l. Data Mining Impact Assessment

7: Written Privacy Complaints

Indicate the number of written complaints for each type of privacy issue received by the SAOP or others at the organization

7a. Process and Procedural — consent, collection, and appropriate notice

7b. Redress — non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters

7c. Operational — inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction

7d. Referrals — complaints referred to another organization with jurisdiction

8: Policy Compliance Review

8a. Does the organization have current documentation demonstrating review of the organization's compliance with information privacy laws, regulations, and policies?

8b. Can the organization provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews?

8c. Does the organization use technologies that enable continuous auditing of compliance with stated privacy policies and practices?

8d. Does the organization coordinate with the organization's Inspector General on privacy program oversight?

9: SAOP Advice and Guidance

Please select "Yes" or "No" to indicate if the SAOP has provided formal written advice or guidance in each of the listed categories, and briefly describe the advice or guidance if applicable.

9a. Organization policies, orders, directives, or guidance governing the organization's handling of personally identifiable information

9b. Written agreements (either interagency or with non-Federal entities) pertaining to information sharing, computer matching, and similar issues

9c. The organization's practices for conducting, preparing, and releasing SORNs and PIAs

9d. Reviews or feedback outside of the SORN and PIA process (e.g., formal written advice in the context of budgetary or programmatic activities or planning)

9e. Privacy training (either stand-alone or included with training on related issues)

10: Agency Use of Web Management and Customization Technologies

(e.g., “cookies,” “tracking technologies”)

10a. Does the organization use web management and customization technologies on any web site or application?

10b. Does the organization annually review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance?

10c. Can the organization demonstrate, with documentation, the continued justification for, and approval to use, web management and customization technologies?

10d. Can the organization provide the notice language or citation for the web privacy policy that informs visitors about the use of web management and customization technologies?

10e. Number of requests for Tier 3 web measurement and customization technologies approved by the SAOP during the reporting period (see OMB M-10-22 for more information)

11: Information System Security

11a. Number of authorizations to operate (ATOs) or reauthorizations issued during the reporting period

11b. Number of ATOs or reauthorizations approved by the SAOP during the reporting period (OMB M-14-04 provided that SAOP approval is required as a precondition for the issuance of an ATO)

12: Breach Response and Notification

Pursuant to FISMA, each federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems. New US-CERT Federal Incident Notification Guidelines are effective October 1, 2014.

12a. Number of confirmed breaches reported by your organization to the U.S. Computer Emergency Readiness Team (US-CERT) during the reporting period

12b. Number of confirmed non-cyber related (e.g., paper) breaches experienced by your organization during the reporting period (OMB M-15-01 provided that non-cyber related incidents should be reported to your agency’s privacy office and not to US-CERT)

12c. Number of persons potentially affected by all confirmed breaches, both cyber and non-cyber, during the reporting period (approximate figures if precise figures are not available)

12d. Number of potentially affected persons who were provided notification about a breach of information experienced by your organization that occurred during the reporting period