

FY 2012

Senior Agency Official for Privacy
Federal Information Security Management Act
Reporting Metrics

Prepared by:

US Department of Homeland Security

National Cyber Security Division

Federal Network Security

January 31, 2012

FY 2012 Senior Agency Official for Privacy FISMA Reporting

Q1: 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

Q2: PIAs and SORNs

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

Q3: Senior Agency Official for Privacy (SAOP) Responsibilities

- 3a. Can your agency demonstrate with documentation that the SAOP participates in all agency information privacy compliance activities?
- 3b. Can your 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?
- 3c. Can your agency demonstrate with documentation that the SAOP participates in assessing the impact of the agency's use of technology on privacy and the protection of personal information?

Q4: Privacy Training

- 4a. Does your agency 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 agency 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?

Q5: PIA and Web Privacy Policies and Processes

Does the agency 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 agency'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 agency'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 agency web sites (i.e., use of P3P).

Q6: Conduct of Mandated Reviews

Reviews Mandated by the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007

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

Q7: Written Privacy Complaints

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

- 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 agency with jurisdiction

Q 8: Policy Compliance Review

- 8a. Does the agency have current documentation demonstrating review of the agency's compliance with information privacy laws, regulations, and policies?
- 8b. Can the agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews?
- 8c. Does the agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices?
- 8d. Does the agency coordinate with the agency's Inspector General on privacy program oversight?

Q9: 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. Agency policies, orders, directives, or guidance governing the agency'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 agency'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)

Q10: Agency Use of Web Management and Customization Technologies (e.g., “cookies,” “tracking technologies”)

- 10a. Does the agency use web management and customization technologies on any web site or application?
- 10b. Does the agency annually review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance?
- 10c. Can the agency demonstrate, with documentation, the continued justification for, and approval to use, web management and customization technologies?
- 10d. Can the agency provide the notice language or citation for the web privacy policy that informs visitors about the use of web management and customization technologies?