Conducting Privacy On-Site Reviews Procedure

Directive No: CIO 2151-P-07.0

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Conducting Privacy On-Site Reviews Procedure

1. PURPOSE

The purpose of this procedure is to identify the types and frequency of privacy on-site reviews to be conducted by EPA's National Privacy Program. The National Privacy Program will coordinate on-site reviews with Agency information security staff, Information Management Officials (IMO) and Liaison Privacy Officials (LPO), as appropriate, to ensure that the Agency is compliant with its requirements under the Privacy Act and the Federal Information Security Management Act.

2. SCOPE

This procedure applies to all records, systems, applications, and databases that collect, contain, or disseminate personally identifiable information (PII). Individual systems or system categories will be selected for review by the National Privacy Program. All applicable systems will be reviewed within a 4-year time period. These procedures apply to both electronic and paper systems.

3. AUDIENCE

All agency employees and agency contractors that maintain PII data in an EPA system.

4. BACKGROUND

The Privacy Act of 1974, 5 U.S.C. 552a, prescribes requirements for federal agencies to follow to collect, maintain or disseminate information about individuals. Specifically, the Act provides safeguards against unwarranted invasions of privacy resulting from the misuse of records by federal agencies by: (1) restricting disclosure of personal information maintained in a system of records (SOR); and (2) requiring compliance with statutory requirements for collecting, maintaining, using and disseminating records.

The Office of Management and Budget Circular A-130, Appendix I, describes agency responsibilities for implementing the reporting and publishing requirements of the Privacy Act. All federal agencies must conduct the reviews listed under Section 6 of these procedures. This procedure identifies the required Privacy Act reviews and how often each review will be conducted. Guidance documents will be issued by the National Privacy Program detailing the specifics for conducting the review types.

5. AUTHORITY

- Privacy Act of 1974, 5 USC 552a (1974)
- Federal Information Security Management Act (FISMA) (Public Law 107-347, 44 U.S.C. § 3541)
- E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36)
- OMB Circular A-130, Appendix I

6. PROCEDURE

The Agency Privacy Officer will provide instructions to IMOs and LPOs for conducting Privacy Act reviews as set forth in Appendix I to OMB Circular 130. Federal agencies are required to conduct the following reviews:

1. **Contracts**. A sample of agency contracts that provides for the maintenance of a SOR on behalf of the agency will be reviewed every two years to ensure that the wording in each contract makes the provisions of the Privacy Act binding on the contractor and its employees.
2. **Recordkeeping Practices**. Agency recordkeeping and disposal policies and practices will be reviewed every two years to ensure compliance with the Act, with special emphasis on the management of automated records.
3. **Routine Use Disclosures**. Routine use disclosures will be reviewed every four years to ensure that the recipient's use of such records continues to be compatible with the purpose for which the Agency collected the information.
4. **Exemption of SOR**. Exemption reviews will be conducted every four years to determine whether an exemption for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Act is still needed.
5. **Privacy Act Training**. Privacy Act training will be reviewed every two years to ensure that all agency personnel are familiar with the requirements of the Act, the agency's implementing regulations, and any special requirements of their specific jobs.
6. **Privacy Act Violations**. Privacy Act violations will be reviewed every two years to ensure that the actions of agency personnel that have resulted in EPA being found civilly liable under the Act, or an action by an employee having been found criminally liable under the Act, are being addressed to determine the extent of the problem and to find the most effective ways to prevent a reoccurrence.
7. **SOR Notices**. Agency SOR notices will be reviewed every two years to ensure that they accurately describe the system and where changes are needed, that an amended notice is published in the Federal Register.
8. **Implementation Plans for Reducing PII Holdings and Social Security Numbers (SSN)**. Plans for reducing PII holdings will be reviewed annually for records/systems/programs that collect, maintain, and disseminate PII to determine if elements are still needed, especially SSNs.
9. **Matching Programs**. Any computerized comparison of two or more automated systems of records between federal agencies or between a federal and non-federal agency. Programs will be reviewed annually to ensure that the requirements of the Act, the OMB guidance, and any Agency regulations, operating instructions, or guidelines have been met.

7. ROLES AND RESPONSIBILITIES

Information Management Officials (IMOs) - Ensure that LPOs carry out their privacy responsibilities and report to the Senior Information Official on privacy initiatives and implementation requirements to ensure that information systems comply with Privacy Act requirements.

Information Security Officers (ISOs) – Perform periodic reviews of existing systems and databases to determine if PII data elements are still required, and if so, that they are adequately protected, and if not, to ensure they are properly removed.

- Terminate systems when no longer maintained in accordance with proper destruction/transfer procedures.
- Ensure that the policies for managing systems with sensitive PII is followed.
- Ensure system users are properly trained.

Liaison Privacy Officials (LPOs) – Prepare for on-site reviews, respond to review findings and take corrective measures, if necessary.

- Assist Privacy Officer with conducting on-site reviews.
- Address the results of on-site reviews, as necessary.
- Conduct ad hoc reviews and report findings to the Privacy Officer.
- Review Privacy Threshold Analyses and Privacy Impact Assessments (PIA), as required.

Privacy Officer – Implements, reviews, analyzes and reports on the results of privacy on-site reviews to the Senior Agency Official for Privacy (Assistant Administrator, Office of Environmental Information). The Privacy Officer:

- Selects the system/program to be reviewed.
- Prepares documentation to support the on-site review.
- Initiates the review.
- Coordinates on-site reviews with the Liaison Privacy Official.
- Analyzes results.
- Reports findings, as appropriate.
- Provides feedback to offices and regions.

Senior Information Official (SIO) – Responsible for privacy compliance including making appropriate changes in a timely manner to program or regional privacy policies and procedures based on the monitoring and oversight results and recommending changes to Agency level policies and procedures as appropriate.

System Owner(s) – Responsible for the development and/or maintenance of a system (paper or electronic).

- Prepares privacy documentation for new and revised systems.
- Works with record liaison officers to ensure that systems/records are covered under the appropriate records control schedule.
- Prepares PIAs for any system that collects PII in coordination with the ISO or LPO, as appropriate.
- Identifies alternatives for using SSNs in systems.

8. RELATED INFORMATION

- Privacy Act of 1974 (5 USC 552a) (http://archives.gov/about/laws/privacy-act-1974.html)
- EPA's Privacy Policy (http://www.epa.gov/privacy/policy/index.htm)
- M-01-05, Guidance of Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, December 20, 2005
- M-06-15, Safeguarding Personally Identifiable Information, May 22,2006
- M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006
- M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006
- M-06-25, FY 2006 E-Government Act Reporting Instructions, August 25, 2006
- M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 25, 2007
- M-08-09, New FISMA Privacy Reporting Requirements for FY 2008, January 18, 2008
- M-08-21, FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 14, 2008
- M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, August 20, 2009
- M-10-15, FY2010 Federal Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, April 21, 2010
- Privacy Onsite Review form https://intranet.epa.gov/oms/ei/saiso/Privacy1/docs_guidance.html
- Privacy Policy http://www.epa.gov/privacy/policy/index.htm
- Privacy Threshold Analysis https://intranet.epa.gov/oms/ei/saiso/Privacy1/docs_guidance.html
- Privacy Impact Assessments https://intranet.epa.gov/oms/ei/saiso/Privacy1/docs_guidance.html

9. DEFINITIONS

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual.
Privacy Act. The federal statute that sets forth requirements for agencies to follow when they collect, maintain or disseminate information about individuals.
Privacy Act Information. Data about an individual that is retrieved from federal documents or files by name or other personal identifier assigned to the individual.
Privacy Impact Assessment (PIA). An analysis of how privacy information is handled: (i) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privacy Threshold Analysis (PTA). A survey of questions that is prepared for all new systems and any other systems that undergo substantial modifications. The PTA

determines if the system will be collecting any PII data elements and if a full PIA is required to evaluate privacy risks from the collection. Review of survey responses will allow the Privacy Act Officer to determine whether any personally identifiable data elements will be collected and whether a full PIA is required.
Record. Any item, collection or grouping of information about an individual maintained by an agency (e.g., an individual's education, financial transactions and medical, criminal or employment history; and that contains the individual's name, or any identifying number, symbol or particular assigned to the individual).
Routine Use. Any outside disclosure of Privacy Act information in which the use is compatible with the purpose for which the information was collected. Routine uses must be included in the published notice for the SOR involved.
System Categories. Grouping of systems that share common characteristics such as Privacy Act system of records (SORs), systems that contain or collect sensitive PII, systems that contain or collect non-sensitive PII, systems that collect PII from the public, etc.
System of Records (SOR). 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.

10. WAIVERS

None.

11. MATERIAL SUPERSEDED

None.

12. CONTACTS

For further information, please contact the Office of Information Security and Privacy, Office of Mission Support or visit
https://usepa.sharepoint.com/sites/oei_Community/OISP/Privacy

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2020.09.28 10:57:39 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency