NOAA Privacy Impact Assessment Guidance

NOAA OCIO Information Technology Standard

Title:	NOAA PRIVACY IMPACT ASSESSMENT GUIDANCE		
Current Version Date:	February 11, 2008		
Effective Date:	02-11-2008	Expiration Date:	
Originator:	Sarah Brabson	Current Editor:	Sarah Brabson

TABLE OF CONTENTS

KEYWORDS

Personally identifiable information (PII), Privacy Impact Assessment (PIA), IT system, records

PURPOSE AND SCOPE

A PIA is a process for determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting information in identifiable form.

A Privacy Impact Assessment must be completed for any IT system containing personally identifiable information (e.g. name and/or contact information, financial information, date of birth and/or SSN) for any individuals *including* federal employees. NOTE: On December 12, 2007, DOC issued a memo requesting additional information regarding technical controls: *The system owner should describe his/her process for logging/monitoring data extracts, including the process for reviewing the logged information to determine: 1) how it is used, and 2) if there is still a need for it after 90 days (such extracts must be destroyed after 90 days if no longer needed). If the logging/monitoring process is automated, the system owner can describe the process used for implementing NIST-800-53 Rev 1, Security Controls for Auditable Events (AU-2,"Auditable Events", AU-3,"Content of Audit Record", AU-6, "Audit Monitoring, Analysis and Reporting" and AU-11, "Audit Record Retention"). The system owner should include the requirement to verify that PII extracts are logged, verified and erased within 90 days in the auditable events criteria in AU-2 and AU-1.* This request has been added to the NOAA PIA Template.

For systems under DOC, a second trigger for a PIA is business identifiable information: "trade secrets and commercial or financial information obtained from a person that is privileged or confidential" (Privacy Act of 1974, 5 U.S.C 552(b)(4)).

A PIA should be submitted as soon as possible when it is determined that one is required (e.g. through a Privacy Threshold Analysis as part of a Certification and Accreditation). PIA submissions are coordinated by the NOAA Paperwork Reduction Act Clearance Officer/OCIO Privacy Coordinator, Sarah Brabson (Sarah.Brabson@noaa.gov or 301-713-3333 ext 204).

Scope of this Standard: Guidance

Intended Use of this Standard: Procedure and template

AUTHORITY

1. **1. The Privacy Act of 1974 (5 USC 552a) regulates the Federal Government's collection, use, maintenance, and dissemination of information about individuals.**
2. **Section 208 of the E-Government Act of 2002 (44 USC 36) establishes procedures to ensure the privacy of personal information in electronic records.**
3. **The Paperwork Reduction Act (PRA) of 1995 (44 USC 3501 et seq.) is designed to reduce the public's burden of answering unnecessary, duplicative, and burdensome government surveys.**
4. **The Trade Secrets Act (18 USC 1905) provides criminal penalties for the theft of trade secrets and other business identifiable information.**
5. **The Children's Online Privacy Protection Act of 1998 (15 USC 6501-06) regulates the online collection and use of personal information provided by and relating to children under the age of 13.**
6. **OMB Circular A-130, "Management of Federal Information Resources," establishes a policy for the management of Federal information resources, including automated information systems.**
7. **OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003, provides specific guidance to agencies for implementing Section 208 of the E-Government Act.**
8. **Department of Commerce IT Privacy Policy provides a guidance, definitions, and background regarding PIAs.**
9. **Department of Commerce IT Security Policy Update: Revisions to the DOC *IT Security Program Policy and Minimum Implementation Standards*.**

INTENDED AUDIENCE

- Chief Information Officers
- IT Security Officers
- Project Managers
- Exhibit 300 Managers

DESCRIPTION

Supporting documents:

- Example/Template: http://www.cio.noaa.gov/itmanagement/PIA_NOS_WAS_final_appvd8-29-07.doc
- Documents listed under “Authority”, accessible through links (above).

This subject of policy or guidance falls into the category: Privacy.

DEFINITIONS

Personally identifiable information (PII)

Personally identifiable information (PII) is information that identifies individuals directly or by reference. Examples include direct references such as name, address, social security number, and e-mail address. It also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.

Business identifiable information (BII)

For the purpose of this guidance, business identifiable information (BII) consists of:

(a) Information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity.

Or

(b) Commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)

Privacy Act System of records/system of records notice:
Any system of records as defined in section (a)(5) of the Privacy Act (" . . .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") and noted in the FEDERAL REGISTER either by the Department of Commerce or by another Federal agency.

GUIDANCE

1. It is determined by the NOAA PRA Clearance Officer (NOAA) or the administrator of an IT system – either through consultation with line office and/or OCIO administrators or as part of a C&A process (Privacy Threshold Assessment determines that the system contains PII) – that a PIA is required.
2. NOAA will provide the administrator with the DOC template/example and work with him/her to develop a draft PIA for submission to DOC.
3. The PIA must document the following elements:
   A. Identifying information, including the OMB Exhibit 300 identification number; name of system or OMB information collection control number; related Privacy Act System of Records notice; and name, e-mail address, and phone number of a contact person.
   B. Brief description of the system, its purpose, and the nature of the data that are to be protected.
   C. Event or reason the PIA was conducted (e.g., new data collection, ongoing data collection, or reuse of existing data).
   D. The law or regulation that authorizes the collection and maintenance of the information.
   E. What information is being collected, maintained, or disseminated (e.g., nature and source).
   F. Why the information is being collected, maintained, or disseminated (e.g., to determine eligibility).
   G. Intended use of the information (e.g., to verify existing data).
   H. With whom the information will be shared (e.g., another agency for a specified programmatic purpose).
   I. What opportunities individuals or businesses have to decline providing information in the case of voluntary collections.
   J. What opportunities individual or businesses have to consent to particular uses of the information and how they can grant consent.
   K. How the information will be secured (e.g., administrative and technological controls), including a new requirement "Data Extract Log and Verify": *The system owner should describe his/her process for logging/monitoring database extracts, including the process for reviewing the logged information to determine: 1) how it is used, and 2) if there is still a need for it after 90 days (such extracts must be destroyed after 90 days if no longer needed). If the logging/monitoring process is automated, the system owner can describe the process used for implementing NIST-800-53 Rev 1, Security*

Controls for Auditable Events (AU-2,"Auditable Events", AU-3,"Content of Audit Record", AU-6, "Audit Monitoring, Analysis and Reporting" and AU-11, "Audit Record Retention"). The system owner should include the requirement to verify that PII extracts are logged, verified and erased within 90 days in the auditable events criteria in AU-2 and AU-1.

L. Whether the collection will result in the creation of a system of records within the meaning of the Privacy Act (*see #4 below*).

M. The records retention period, under the applicable General Records Schedule.

The depth and content of the PIA statement should be commensurate with the size of the information system being assessed, the sensitivity of the information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information. For example, PIA statements for major information systems will reflect more extensive analyses of the consequences of the collection and flow of information; the alternatives to collection and handling as designed; privacy risk mitigation measures for each alternative; and the rationale for the final design choice or business process.

4. (If it is determined by NOAA that a system of records notice (SORN) must be written, i.e. if files in the system are retrievable by any of the PII or BII elements, then NOAA provides the IT administrator with the template and refers him/her to the NOAA Privacy Act Officer (if a NMFS system, the first referral is to the NMFS Privacy Act Officer). *The NOAA OCIO Privacy Coordinator does not participate in review of the notice, but tracks its progress through NOAA and DOC).*
5. The completed draft PIA is routed through the Line Office ITSO to the NOAA CIO Privacy Coordinator.
6. The draft PIA is forwarded by NOAA to Dan Rooney, DOC, who requests any needed clarifications or additional detail.
7. NOAA consults with the IT administrator on changes requested by DOC and sends a revised draft to DOC.
8. Step 6 is repeated if DOC requests further changes.
9. If no further changes are requested by DOC, DOC approves the PIA.
10. NOAA posts the approved PIA on the PIA page on the NOAA OCIO website: http://www.cio.noaa.gov/itmanagement/PIA.html.
11. DOC maintains a link to this page on its IT Privacy page: http://www.osec.doc.gov/cio/oipr/it_privacy_page.htm.