



# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, D.C. 20240

OCIO BULLETIN 2002 - 015

OCT 18 2002

To: Solicitor  
Inspector General  
Heads of Bureaus and Offices  
Bureau/Office Chief Information Officers  
Bureau /Office Deputy Chief Information Officers

From: W. Hord Tipton  
Chief Information Officer

Subject: Privacy Impact Assessments for Department of the Interior Information Systems

## **Purpose:**

This bulletin and the attached Department of the Interior (DOI) Privacy Impact Assessment (PIA) and Guide (see Attachment I) provide new policy and guidance to system owners and developers that will help in identifying privacy risks and integrate privacy protections into new and modified information systems containing personal information. The Office of Management and Budget (OMB) now require the PIAs with Exhibit 300 budget submissions, and for the DOI Information Technology (IT) Security Certification and Accreditation (C&A) process.

Because OMB just recently included PIAs as a requirement (see OMB Circular A-11), this office was not able to pilot the attached document. Therefore, the attached version of the PIA and Guide will be used on a temporary basis and will be open for comment for the next three months. Comments should be sent to the contact listed below during that time.

## **Background:**

As the implementation of electronic information collection and sharing capabilities increases to support Government agency mission and functions, so does the public and Governmental concern over the use, or potential misuse of personal information contained in these systems. The PIA is a new Government requirement to ensure that system owners and developers consider and evaluate existing statutory and key information management requirements that must be applied to new or modified Government systems that contain personal information. Going through the PIA process will also help to identify sensitive systems so that appropriate information assurance measures are in place, such as secured storage media, secured transmission and access controls.

The benefits from building in privacy protections into information systems include enabling the Department to be a good steward of entrusted personal information and its information resources; increasing DOI's customers confidence in providing personal information to DOI; eliminating expensive costs of modifying information systems to include privacy protections after system implementation, and protecting the DOI technology investment.

The Federal Chief Information Officer (CIO) Council endorsed the Internal Revenue Service (IRS) PIA in 2000 as a Government-wide "Best Practice" and encouraged that Government agencies develop and use similar assessments. The Department of the Interior CIO recommended the use of a PIA in CIO Bulletin No. 2001-002, Guidance on Inter-Agency Sharing of Personal Data, and Privacy Protection Measures in System Development and Applications, February 26, 2001, at <http://www.doi.gov/ocio/bulletins/2001-02bul.htm>.

Although completing a PIA was previously voluntary, the OMB now requires that a PIA be completed and submitted with Capital Asset Planning document, Exhibit 300, for budget submissions (see OMB Circular A-11, sections 31.8, 53.1, and 300.9). In addition, a completed PIA is now required for the DOI IT Security C&A process.

The Office of the CIO prepared the attached "PIA and Guide" that is based on the IRS PIA. This document brings together privacy requirements for information systems from the Privacy Act, Computer Security Act, the Clinger-Cohen Act, the Government Paperwork Reduction Act, the Freedom of Information Act, and OMB Circulars A-130: Management of Federal Information Resources and A-123: Management Accountability. A sample of a completed PIA is provided in Attachment II.

**Scope:**

The requirements identified in the DOI PIA must be considered early when planning, developing, implementing, and modifying individual agency information management systems that contain personal information (this applies not only to Privacy Act systems of records where personal information is retrieved by the subject's name or other identifier, but any system that contains personal information). New and modified systems also include those created by extracting data from an existing system that alters the purpose for which the information is used; those created from combining data from two or more existing systems; and systems created from information collected from individuals off DOI web pages.

If personally identifiable information is paired with geographic information and related spacial data, PIAs must be completed for these systems as well. The revised OMB Circular A-16 on "Coordination of Geographic Information and Related Spacial Data Activities" dated August 19, 2002 also requires that those agencies that collect, use, or disseminate geographic information and/or carry out related spacial data activities also comply with Government law and policy on privacy protection (see 2.a. and 8.a.7 of the Circular).

In cases where systems are networks that house information systems and do not actually collect, manipulate, or use the data in the systems they house, and where systems are evaluated and no personally identifiable information is found, complete Sections A and B.1 of the PIA. Attach this analysis to the Exhibit 300 and IT Security Certification to certify that a review for any personally identifiable information in the system was made.

The system owner and developer will need to coordinate certain responses to questions in the PIA with the bureau/office Privacy Act Officer, IT Security Manager, Records Officer, and appropriate management, if necessary, and obtain signature approval.

**Time Frame:**

This bulletin and the requirements for completing PIAs will become effective immediately and will remain in effect indefinitely. The PIA and Guide document will be open for comment for a period of three months from the date of this bulletin.

**Policy:**

The PIA is required for new or modified systems that collect, use, or access personally identifiable information when they require a Capital Asset Plan Exhibit 300 or Information Technology Security C&A. For new or modified systems, which do not require an Exhibit 300 or C&A, it is recommended that a PIA be used to ensure that measures are in place to protect privacy in all DOI information systems that contain personal information.

**Contact:**

For questions and comments on the PIA and Guide, please contact Marilyn Legnini, Departmental Privacy Act Officer, Office of the CIO, at 202-219-0868. If you have any questions concerning the Privacy Act, contact your bureau/office Privacy Act Officer for specific guidance. A list of bureau/office Privacy Act points-of-contact is available at: [http://www.doi.gov/ocio/privacy/doi\\_privacy\\_act\\_officers.htm](http://www.doi.gov/ocio/privacy/doi_privacy_act_officers.htm).

Attachments

cc:  
IT Security Managers  
DOI Privacy Act Officers