# Privacy Impact Assessment (PIA)

## Privacy Impact Assessments (PIA)

* [Office of the Secretary PIAs](file:///C:\DOCPUB%20WEB\opog\privacy\words\os-pias.html)
* [Census Bureau PIA Guide](http://www.census.gov/privacy/pia/guide_to_ds-pias.html) and [PIAs](http://www.census.gov/privacy/pia/list_of_available_pias.html)
* [US Patent and Trademark PIAs](http://www.uspto.gov/web/doc/privacy_pia.htm)
* [National Oceanic and Atmospheric Administration PIAs](http://www.cio.noaa.gov/Policy_Programs/PIA.html)
* [Economic Development Administration Revolving Loan Fund Mgmt. System](http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/ssLINK/PROD01_001988)
* [International Trade Adminstration Foreign Trade Zones Board PIA](http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/ssLINK/PROD01_005192)
* [National Institute of Standards and Technology](http://www.nist.gov/director/oism/policies.cfm)

## What is a Privacy Impact Assessment (PIA)?

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.

The E-Government Act requires that agencies conduct a PIA before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form or (ii) initiating a new electronic collection of information that will be collected from 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government, and will be maintained, or disseminated in an identifiable form, using information technology.

PIAs are conducted to ensure that there is no collection, storage, access, use, or dissemination of identifiable information from or about members of the general public and businesses that is not needed or authorized, and that identifiable information that is collected is adequately protected. PIAs may address issues relating to the integrity and availability of data handled by a system, to the extent these issues are not already adequately addressed in a System Security Plan.

Operating units should begin the PIA process when they propose a new IT system through the budget process that will collect, store, or process identifiable information or when starting to develop or significantly modify such a system, or when a new electronic collection of identifiable information is being proposed. The conduct of a PIA is a multidisciplinary process, and operating units should coordinate the efforts of system managers as well as experts in information technology, security, and privacy law and policy in determining whether a PIA should be conducted and in drafting PIAs. The system manager and the system developer must work together to conduct the PIA. The system manager must address what data are to be collected or processed, how the data will be used, and who will be authorized to use the data. The system developer must address what system protections are being applied or will be applied to ensure adequate protection of the data.

To conduct an effective and comprehensive PIA, the system manager and developer should include in the review process those individuals who have expertise in the program area, legal issues, privacy, records management, human resources, and any other subject matter area that may be applicable to the system under review.

## For what systems or information collections must a PIA statement be completed?

PIA statements must be completed for new systems and proposed information collections that contain personally identifiable information, including systems under development and systems undergoing major modifications.

PIA statements must be developed for all investigative, law enforcement case files, and human resources databases even if they were previously exempt because they have not been modified or contained information only about federal employees.

PIA statements must also be developed for any legacy systems containing PII for which a current PIA is not in force and up to date. These requirements expand upon those in OMB implementing guidance for the E-Government Act ( [OMB Memorandum M-03-22](http://www.whitehouse.gov/omb/memoranda/m03-22.html)), and in the previous Commerce IT Privacy Policy (July 30, 2004). This policy requires operating units to conduct a PIA before developing or procuring IT systems or investments that collect, maintain, or disseminate information in identifiable form from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new or significantly revised electronic collection of information in identifiable form.

Commerce extends the requirement for PIA statements to systems or collections of information that include business identifiable information before:

* Developing or procuring IT systems or investments that collect, maintain, or disseminate information in identifiable form from or about companies or other business entities.
* Initiating the collection, maintenance, or dissemination of information in identifiable form about companies or other business entities.

Commerce policy also extends the requirement for PIA statements to systems or information collections of personally identifiable or business identifiable information that are:

* Part of new multi-agency projects in which Commerce or a Commerce operating unit is a participant.
* Created, operated, or performed on a reimbursable basis by Commerce for another federal agency under an Interagency Agreement.

All PIA statements must specifically describe how the data extract log and verify requirement of [OMB Memorandum M-07-16](http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf), Safeguarding Against and Responding to the Breach of Personally Identifiable Information, has been implemented for the system.

All PIA statements are also required to be updated where a system change creates new privacy risks. Examples include:

* When a paper based records system is converted to an electronic system.
* When an existing electronic system is modified so that previously anonymous information becomes identifiable.
* When new uses of an existing IT system, such as the application of new technologies, significantly change how identifiable information is managed in the system.
* When databases holding identifiable information are merged, centralized, matched with other databases, or otherwise significantly manipulated.
* When user-authenticating technology (e.g., password, digital certificate, or biometric) is newly applied to an electronic information system accessed by members of the public.
* When agencies systematically incorporate into existing IT systems databases of information in identifiable form purchased from commercial or public sources.
* When agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form.
* When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of identifiable information.
* When new identifiable information that is added to the system increases the risks to personal privacy (e.g., the addition of medical or financial information).
* When a system with identifiable information is relocated to a remote site or a facility not under the direct control of the Department (e.g., a contractor’s processing facility).

In addition, operating units may conduct discretionary PIAs as they determine to be appropriate and necessary.

## Questions and Comments

Send Questions and Comments to [CPO@doc.gov](mailto:CPO@doc.gov).