Commerce Privacy Mission Statement

The Department of Commerce (DOC) is committed to safeguarding personal privacy. Individual trust in the privacy and security of PII is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information-management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy considerations in all systems, programs, and policies.

Key Privacy Laws and Other Guidance

The Department of Commerce adheres to federal privacy laws and guidance to ensure that the collection, use, and maintenance of sensitive information, such as personally identifiable information (PII) and business identifiable information (BII), is properly safeguarded.

Privacy Regulations:

- Freedom of Information Act (FOIA) – 5 U.S.C. § 552
- Privacy Act of 1974 – 5 U.S.C. § 552a
- The E-Government Act of 2002
- Trade Secrets Act – 18 U.S.C. § 1905
- Federal Information Security Modernization Act of 2014 - Public Law No. 113-283
- Paperwork Reduction Act of 1995 (PRA)

Guidance:

- OMB Memorandums M-03-22, M-10-22, M-10-23, M-11-02, M-16-04, M-16-14, M-17-06, M-17-12
- Department of Commerce IT Privacy Policy

Office of Privacy & Open Government

Privacy Program

Privacy Impact Assessments (PIAs)

Section 208 of the E-Government Act of 2002 requires agencies to conduct a Privacy Impact Assessment (PIA) before (1) developing or procuring Information Technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Office of Privacy and Open Government

Email: cpo@doc.gov

DEFINITIONS

Information in identifiable form – information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Information technology (IT) – as defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

PRIVACY THRESHOLD ANALYSIS (PTA)

A PTA is used to determine if a system contains PII, whether a PIA is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system.

SPECIAL NOTE: The Department of Commerce privacy policy includes PII about employees/contractors and Business Identifiable Information (BII).

PRIVACY IMPACT ASSESSMENT (PIA)

A PIA is an analysis of how information is handled: (i) to ensure 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.

PIAs must analyze and describe the following:

- what information is to be collected (e.g., nature and source);
- why the information is being collected (e.g., to determine eligibility);
- intended use of the information (e.g., to verify existing data);
- with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
- what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
- how the information will be secured (e.g., administrative and technological controls); and
- whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

A PIA must be updated to reflect changed information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form, in addition to where a system change creates new privacy risks, such as:

- Conversions
- Anonymous to non-anonymous
- Significant system management changes
- Significant merging
- New public access
- Commercial sources
- New Interagency uses
- Internal flow or collection
- Alteration in character of data

Please refer to The Office of Management and Budget Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, for additional information. This guidance can be found at: https://www.whitehouse.gov/omb/memoranda_m03-22/

PIA PROCESS*

1. System Owner (SO)/Information System Security Officer (ISSO) completes PTA.
2. a) If PTA determines a PIA is not required, SO/ISSO sends PTA to BCPO (Bureau Chief Privacy Officer) or designee for inclusion into the Assessment and Authorization (A&A) package.
   b) If PTA determines a PIA is required, SO/ISSO completes PIA and Controls Assessment Worksheet (CAW) and submits to BCPO/designee.
3. Once approved by BCPO/designee, BCPO/designee submits PTA, PIA, and CAW to DOC Privacy (CPO@doc.gov) for review.
4. DOC Privacy will determine if a Compliance Review Board meeting is required or if the re-certification process can be used.
5. Once approved by DOC Privacy, DOC Privacy submits to Senior Agency Official for Privacy (SAOP) for review and approval.
6. Once approved by SAOP, BCPO/designee will receive approved PIA for posting to website.
7. BCPO/designee will send DOC Privacy confirmation of posting.

*Please confirm with BCPO/designee if additional steps are required for your bureau's internal PIA process.