

The Data Stewardship Program

Policy on Conducting Privacy Impact Assessments

PURPOSE

The purpose of this policy statement is to indicate the requirements for: conducting, updating and releasing a Privacy Impact Assessment (PIA); PIA scope and content; and major roles and responsibilities. There are several legal authorities that establish the requirement for PIAs. These authorities address the importance of agencies protecting identifiable data. The Census Bureau depends on the trust and cooperation of the public to achieve its mission. Compliance with all legal authorities and ethical responsibilities strengthens the relationship with respondents and stakeholders.

LEGAL AUTHORITIES

The following legal authorities and Census Bureau policies and regulations provide a foundation for this policy:

- E-Government Act of 2002
- Office of Management and Budget (OMB) Memorandum 03-22
- Department of Commerce (DOC) Information Technology (IT) Privacy Policy
- OMB Circular A-11, Part 7, Section 300, Planning, Budgeting, Acquisition, and Management of Capital Assets
- Paperwork Reduction Act of 1995
- Homeland Security Presidential Directive (HSPD) 12 and related Federal Information Processing Standards Publication 201 (FIPS Pub 201), Personal Identity Verification (PIV) of Federal Employees and Contractors
- OMB Memorandum 01-05 Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- Privacy Act of 1974
- National Institute of Standards and Technology Special Publication 800-26.

SCOPE

A Census Bureau program, project or system must be covered by an up-to-date privacy impact assessment if it involves the use of identifiable data from or about members of the public and in other cases as required by law or regulation.

BACKGROUND

In December 2002, the E-Government Act of 2002 became law. Section 208 of the Act requires that agencies conduct a PIA when personally identifiable data are involved in a data collection or information

The Data Stewardship Program

technology system that meets certain criteria. The law also specifies, broadly, the areas a PIA should cover, such as what data are involved and uses. Following the implementation of the E-Government Act, OMB issued M-03-22, which provides guidance on implementing Section 208 of the Act. OMB's guidance identifies a number of "triggers" that determine when a PIA should be conducted. Memorandum M-03-022 requires that PIAs be conducted on new electronic collections consistent with the Paperwork Reduction Act (PRA) of 1995. The Paperwork Reduction Act of 1995 requires that agencies obtain OMB approval for new collections of information. The DOC issued a policy in 2004 that extends the legal requirement to identifiable business data and adds a review and clearance requirement with the Office of the Chief Information Officer (CIO). OMB Circular A-11, Part 7, Section 300 requires that PIAs be conducted on major initiatives requesting funding through the OMB Exhibit 300. The HSPD-12 requires PIAs for the PIV systems. OMB M-01-05 reminds federal agencies of the requirements of data sharing and extends guidance to include PIAs as applicable.

The Census Bureau began preliminary work on PIAs long before it was a requirement, incorporating guidance as it became available. PIAs are an important tool for assuring Census Bureau census and survey respondents, other agencies from whom we receive data, and the taxpayer, that the Census Bureau is minimizing privacy impacts and ensuring data confidentiality and security. The PIA tool does this by assessing adherence to the complete set of Census Bureau Privacy Principles that are based on the Organization for Economic Cooperation and Development's (OECD's) Privacy Principles and the fair information principles of the Privacy Act of 1974, and related Census Bureau data stewardship policies. The PIA review tool addresses each phase of program life-cycle development defined as concept, proposal, authorization, planning/organizing, design, collection, processing, analyzing, and archiving.

POLICY

Privacy impact assessments must be conducted when an existing information technology system or a data collection containing identifiable information (person or business) is substantially modified thereby creating new privacy risks, or, a new system or collection is created. A PIA must cover the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system. A PIA must evaluate the protections and alternative processes for handling information to mitigate potential privacy risks. A PIA must use the approved Census Bureau template tool, including a summary statement. The cognizant program manager, Associate Director, Chief Information Officer (CIO), and Chief Privacy Officer (CPO), must approve a new PIA.

A new PIA will be publicly available unless the program manager successfully petitions the CPO for exclusion. Because of the Census Bureau's commitment to transparency, the CPO's office will attach a justification for release to each PIA sent to the DOC CIO as required by the DOC IT Privacy Policy.

Existing PIAs must be updated annually as part of the OMB Exhibit 300 submission process, the Census Bureau IT Business Planning (ITBP) process, and in accordance with Paperwork Reduction Act (PRA) submissions. PIAs are uniquely identified in OMB Exhibit 300 submissions, IT Business Plans,

The Data Stewardship Program

Information Collection Request (ICRs) as part of the Paperwork Reduction Act submission, and in security assessments as identified in the NIST SP 800-26. PIAs must also be reviewed/considered during the creation/updating of a System of Record (SOR) notice consistent with the Privacy Act.

IMPLEMENTATION

□ RESPONSIBILITIES FOR IMPLEMENTATION

Chief Privacy Officer

The CPO is responsible for the implementation and coordination of all PIAs through the process. The Privacy Office coordinates the design, provides technical assistance and reviews and approves all PIAs. The CPO routes PIAs for approval to the CIO. The CPO coordinates with the DOC CPO and CIO. The CPO reviews Exhibit 300, ITBP and associated PIA information provided from the Information Systems Support and Review Office (ISSRO) and informs the ISSRO of any omissions. The CPO follows-up with the PIA contacts to ensure they provide updated Exhibit 300, ITBP and/or PIA information to the ISSRO.

Approximately one month before the deadline for OMB Exhibit 300s or ITBPs to be finalized, the CPO will follow-up with PIA contacts to inform them that their OMB Exhibit 300s or IT Business Plans may be held pending a complete/accurate PIA. The ISSRO will be copied on this communication. The CPO also provides guidance and input into the DS Awareness effort and coordinates SOR notice reviews.

Once the CPO approves the PIA, it will be forwarded to the ISSRO. The ISSRO will provide these PIAs to the CIO along with the ITBP approval letters. The CPO will provide a list to the ISSRO showing the ITBPs associated with each PIA. Once the CIO approves, the CPO will forward the PIA to the Department of Commerce for approval.

PIA Contacts/Owners

PIA contacts are responsible for coordinating with the persons in their area responsible for OMB Exhibit 300s, IT Business Plans, Information Collection Requests, and SP 800-26 security assessments to ensure all documents correctly cross-reference the applicable PIA and vice versa. PIA Contacts are responsible for getting the PIA reviewed internally and approved by their Associate Director. Once approved, the PIA contact should forward the PIA to the Privacy Office for review and approval by the CPO and CIO.

The Data Stewardship Program

Office of Analysis and Executive Support

The Office of Analysis and Executive Support (OAES) advises the CPO on design considerations as Data Stewardship (DS) policies are developed and updated. The OAES is responsible for submitting policies through the standard review approval process. The office also publishes the policies on the Census Bureau Intranet and manages the DS Awareness effort.

Information Systems Support and Review Office

The ISSRO provides program areas with basic information on the requirements for PIAs. The ISSRO sends the CPO a list of Exhibit 300s and ITBPs with PIA information for review. The CPO informs the ISSRO of any omissions and follows-up with the PIA contact to ensure they send updated information to ISSRO. If an ITBP requires a PIA, the ISSRO will withhold approval of the ITBP until the CPO has provided the ISSRO with a complete PIA. The ISSRO will send the ITBP and completed PIA to the CIO for approval. The ISSRO will send the approved PIA back to the CPO for forwarding to the Department of Commerce for approval.

Forms Clearance Officer

The Forms Clearance Officer (FCO) is responsible for providing program areas basic information on the requirements for PIAs. The Forms Clearance Officer will provide PIA information to program areas when preparing the “pre-submission notice” and ensures approved PIAs are included/identified on Forms Clearance Packages in the Supporting Statement.

IMPLEMENTATION and AWARENESS STRATEGIES

The basic implementation strategy consists of modifying existing processes to include the PIA review, approval and submission tasks. The OMB Exhibit 300 and ITBP process is coordinated by the ISSRO who provides basic information in the OMB Exhibit 300 template and process, the ITBP template and process, and conducts meetings with Exhibit 300 and ITBP contacts reminding them to review, update, and submit PIAs as appropriate. The CPO is responsible for providing the ISSRO the updates to the PIA section of the guidance documentation. The FCO includes basic information in the forms clearance guidance. All of these process templates, forms, and guidance are provided online via the Census Bureau Intranet. This policy is also provided online via the Intranet. Additionally, the basic requirements of the policy and process are covered in the DS Awareness program.

IMPLEMENTATION MEASURES

The Data Stewardship Program

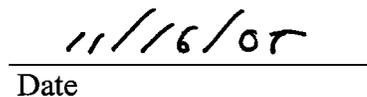
The annual Federal Information Security Management Act (FISMA) report includes Section D that consists of reporting on the number of PIAs required versus the number conducted for each fiscal year. This annual count will inform how well the Census Bureau is meeting the PIA requirement. Section D of this report is completed by the CPO. The decisions or choices made on IT systems or information collections based on the PIA will also be examined as a possible metric of measure.

DATE POLICY BECOMES EFFECTIVE: Upon Signature

SIGNATURE AND DATE SIGNED



Hermann Habermann
Chair, Data Stewardship Executive Policy Committee



Date