Privacy Impact Assessment (PIA)

Summary Description:

The E-Government Act of 2002, Section 208 (Public Law 107-347, 44 U.S.C., Ch 36) requires Federal agencies to conduct a Privacy Impact Assessment (PIA) when "developing or procuring information technology . . . or initiating a new collection of information . . . in an identifiable form . . . " The purpose of a PIA is to ensure there is no collection, storage, access, use or dissemination of identifiable respondent information (i.e., identifiable data about both people and businesses) that is not both needed and permitted. A PIA is an agency review of how collected information is handled by the agency. The review is a program analysis that determines whether the data collected are protected in a manner consistent with Federal standards for privacy and security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. In addition to being required by the E-Government Act of 2002, PIAs are required by Office of Management and Budget (OMB) Circular No. A-11 and OMB Exhibit 300, "Capital Asset Plan and Business Case," which tie together privacy considerations and executive agency funding requests. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data. A PIA is organized around four Privacy Principles: 1) mission necessity, 2) informed consent, 3) protection from unwarranted intrusion, and 4) protection of confidentiality.

Status:

Mandatory - The Department of Health & Human Services (DHHS) requires that a Privacy Impact Assessment (PIA) be prepared for all CMS General Support Systems (GSSs) and Major Applications (MAs), in order to assist the Department in incorporating privacy protections into every stage of an IT system's life cycle. OMB also requires that a PIA be prepared for and approved by OMB for every new information technology-funding request. In order to meet the Department's and OMB's information needs, CMS requires that each system or application that is covered by a GSS or MA prepare a PIA at the individual system or application level.

Timeframe:

Privacy Impact Assessments (PIAs) are prepared on an annual basis in accordance with guidance provided from DHHS and OMB. An initial PIA is conducted for all systems or applications, whether currently in existence, undergoing modification, or being newly developed.

Responsible Reviewing Component:

OIS/EDG/DPCDD is the CMS component that has the primary decision authority over the need for a Privacy Impact Assessment (PIA), the requirements for its creation, and acceptance of the end product in meeting the information needs.

Primary Information Exchange Partners:

The following are the primary stakeholders who have an interest in the Privacy Impact Assessment (PIA):

OIS/PMSG
Privacy Officer
Senior Information Systems Security Officer (ISSO)
Chief Information Officer (CIO)
CMS Administrator
Beneficiary Confidentiality Board (BCB)
DHHS Privacy Act Officer
Office of Management & Budget (OMB)

Government Responsibilities:

The System Owner/Manager and Business Owner(s)/Partner(s) have primary responsibility for preparing the Privacy Impact Assessment (PIA) for a system or application in accordance with the direction provided by OIS/EDG/DPCDD, and for determining whether the security controls that protect their system(s) are adequate enough for operation.

Contractor Responsibilities:

Not Applicable

Content:

The Privacy Impact Assessment (PIA) consists of two documents. The first is a Privacy Analysis Worksheet (PDF), which is a questionnaire that collects all relevant data necessary to provide a solid evaluation of the privacy risks, controls, and requirements of the analyzed system. The second is the PIA Summary (PDF), which is a shorter document that describes the information collected through the Worksheet and is suitable for public release. Because the later document will be available to the public, privacy risks involving system vulnerabilities should be described only in extremely general terms so that information cannot be used to exploit these vulnerabilities.

The information contained in a PIA must be consistent with information contained in the

corresponding System Security Plan (SSP) and/or Information Security Risk Assessment, and if applicable, the corresponding Exhibit 300.

Guidance:

Much of the information included in a Privacy Impact Assessment (PIA) may be included in a System of Records (SOR), which may be a useful reference in the preparation of the PIA. However, a copy of the SOR may not be submitted in place of the PIA.

For additional information and assistance regarding the preparation, formal review and clearance of a PIA, contact OIS/EDG/DPCDD.

Review Process:

The Privacy Impact Assessment (PIA) is reviewed by OIS/PMSG/DIAB, the Senior Information Systems Security Officer (ISSO) and Beneficiary Confidentiality Board (BCB), and signed by the CMS Privacy Officer, Chief Information Officer (CIO), and Administrator, before being submitted to the DHHS Privacy Act Officer and the Office of Management & Budget (OMB).

Date Created/Modified:

September 2004