DISA GUIDANCE FOR CREATING A PRIVACY IMPACT ASSESSMENT (PIA)

Introduction Defense Information Systems Agency recognizes the importance of protecting the privacy of individuals, especially as it modernizes and develops its information technology (IT) systems. Section 208 of the E-Government Act of 2002 establishes Government-wide requirements for conducting, reviewing, and publishing Privacy Impact Assessments (PIA). These assessments explain how the Agency factors in privacy issues for all new or significantly altered IT systems or projects that collect, maintain, or disseminate PII about members of the public –Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally.

In September 2003, the Office of Management and Budget (OMB) issued guidance to agencies implementing the privacy provisions of the E-Government Act. That guidance can be found at http://www.whitehouse.gov/omb/memoranda/m03-22.html. DISA has adopted the requirements prescribed in the OMB guidance, in addition to agency specific requirements, as our official process for implementing DOD PIAs.

Objective

The objective of this document is to provide guidance on how to complete a PIA for your IT system. This guidance is intended for those familiar with the system, such as the System Managers and those who serve in a similar capacity and will be responsible for completing and submitting the PIA The PIA represents a snapshot of the privacy posture of the system at the time the PIA is completed. If in the future the system is modified or upgraded, new data is collected or distributed, or the system is interconnected to other systems, an updated PIA is required to assess the privacy protection posture of the system.

What is a Privacy Impact Assessment?

A Privacy Impact Assessment **(**PIA) is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. Personally identifiable information (PII) is defined as information in a system or online collection that directly or indirectly identifies an individual whether the individual is a member of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally.

Examples of PII that directly identifies an individual - individual's name, date of birth, home mailing address, telephone number, social security number, personal email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, internet protocol addresses, biometric identifiers, photographic facial images, any other unique identifying number or characteristic.

Examples of PII that indirectly identifies an individual - any information where it is reasonably foreseeable that the information will be linked with other information to identify an individual. Data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.

What is the Purpose of the Privacy Impact Assessment?

The purpose of a PIA is to demonstrate that system owners/developers have consciously incorporated privacy protections throughout the entire life cycle of an IT system. The PIA process and the document itself are intended to:

- Ensure that technology choices reflect the incorporation of privacy into the fundamental system architecture from the start, not after the fact when privacy concerns can be far more costly to address or could affect the viability of the project;

- Help the public understand what information DISA is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored.

The PIA is a living document that needs to be updated regularly as the program and system are developed, not just when the system is deployed. In cases where a legacy system is being updated the PIA demonstrates that the system developers and program managers have implemented privacy protections into the updates.

Who Should Conduct a Privacy Impact Assessment?

The Program Manager maybe the best individual to conduct the PIA. DISA official having responsibility for either procuring or developing the IT system or modifying an existing IT system to collect new information in identifiable form.

The responsible official works with the DISA Privacy Officer when trying

(1) to determine if their information collection requires a Privacy Act system of records notice to be published in the *Federal Register;* or

(2) to determine if their information collection may already be covered by an existing DoD/DISA or Government-wide Privacy Act system of records notice (SORN).

- Government-wide Privacy Act systems of records notices are available at http://www.dod.mil/privacy/govwide/ .
- DISA Privacy Act systems of records notices are available at http://www.defenselink.mil/privacy/notices/disa/.

When Should a Privacy Impact Assessment be Conducted?

A Privacy Impact Assessment should be conducted when an office is:

1. developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public public –Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally . A PIA is required for all budget submissions to OMB;
2. initiating a new electronic collection of information in identifiable form for ten or more members of the public public –Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally; or

3. when a system change creates new privacy risks.

Such as:

- when converting paper-based records to electronic systems;
- when changing anonymous information into information in identifiable form;
- when new uses of an IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- when merging, centralizing, or matching databases that contain information in identifiable form with other databases, or when otherwise significantly manipulating such databases;
- performed when PII about members of the public (Reference (c)), Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally, is collected, maintained, used, or disseminated in electronic form.
- when systematically incorporating into existing information systems.

Guidelines for Writing the Privacy Impact Assessment.

PIAs should be written from the perspective of a member of the public who knows nothing about the system or technology. Spell out each acronym the first time you use it in the document. Use words, phrases, or names in the PIA that are readily known to the average person. Technical terms or references should be defined. Clearly reference projects and systems and provide explanations, if needed, to aid the general public. References identified within the PIA should include their complete name the first time they are used. Subsequent references may use an abbreviated format. The link to DISA published PIAs http://www.disa.mil/about/legal/pia/index.html .

What is a Privacy Act System of Records Notice?

A system of records is a group of records under the control of an agency which contains a personal identifier (such as a name, date of birth, finger print, Social Security Number, Employee Number, etc.) and one other item of personal data (such as home address, performance rating, blood type, etc.) from which information is retrieved by a personal identifier. The Privacy Act requires each agency to publish an notice in its systems of records in the *Federal Register* which are called "system of records notice" (SORN).

The SORN must be published in the *Federal Register* BEFORE any information may be collected and maintained; therefore, contact your Privacy Act Office early in the development process. Developing a Privacy Act system of records is not a difficult process, but it can be a lengthy one (sixty days or longer).

The SORN is a living document that needs to be reviewed for accuracy biennially. Contact the DISA Privacy Act Office [703 681-2409] for more information on Privacy Act systems of records notices.

DISA Privacy Impact Assessment
Template

Questions and explanation under each of the required elements are provided to assist in completing your PIA. Complete, comprehensive answers will provide much of the information required to properly address each of the elements contained in the Department of Defense (DoD) format. Please include any additional information you feel will comprehensively address each element at the attached link http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2930.pdf