Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6502.2
Transmittal Sheet
October 21, 2004

PRIVACY IMPACT ASSESSMENT

1. REASON FOR ISSUE: This handbook establishes Department-wide procedures for the Privacy Impact Assessment (PIA), and implements the policies pertaining to the PIA that were set forth in Department of Veterans Affairs (VA) Directive 6502, Privacy Program. In accordance with the provisions of VA Directive 6502, and in order to comply with the requirements of the E-Government Act of 2002 (Pub. L.107-347), the Privacy Service has been established as the central VA office for compliance with the Federal requirements for PIAs.

2. SUMMARY OF CONTENTS: This handbook describes the responsibilities, requirements, and procedures for the completion and the submission of the PIA.

3. RESPONSIBLE OFFICE: Office of Policies, Plans and Programs (005P), Office of the Assistant Secretary for Information and Technology (005).

4. RELATED DIRECTIVE: VA Directive 6502, Privacy Program.

5. RESCISSIONS: None

CERTIFIED BY:

/s/
Robert N. McFarland
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Robert N. McFarland
Assistant Secretary for
Information and Technology

Distribution: RPC: 6002

FD

PRIVACY IMPACT ASSESSMENT

CONTENTS

PRIVACY IMPACT ASSESSMENT

1. PURPOSE AND SCOPE

a. This handbook provides the procedures and requirements for completing Privacy Impact Assessments (PIAs). PIAs are required under the privacy provisions of the E-Government Act of 2002 and the Department of Veterans Affairs (VA) Privacy Program, in VA Directive 6502, Privacy Program paragraph 3.d.(13).

b. The purpose of the E-Government Act of 2002 is to "...develop and promote electronic Government services and processes...and to promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government." The E-Government Act of 2002 and implementing Office of Management and Budget (OMB) guidance require the protection of electronic personal information that is collected, maintained, and handled by Federal agencies (herein referred to as electronic privacy-protected information (PPI)).

c. VA is required to describe how it manages the security and privacy of PPI through the Systems Development Life Cycle (SDLC) of VA Information Technology systems (IT) that maintain information on the public. The PIA is one of the compliance initiatives managed by the Privacy Service to meet this requirement. The Privacy Service shall establish VA requirements and guidance on the development, completion and periodicity of PIAs.

d. This handbook identifies the minimal required elements for VA PIAs.

2. RESPONSIBILITIES

a. **The Assistant Secretary for Information and Technology**. The Assistant Secretary for Information and Technology, as the Department's CIO, shall review and approve the PIAs along with the Exhibit 300s, per OMB's instructions, and submit approved PIAs to OMB.

(1) **Director, Privacy Service.** The Director shall establish Department-wide PIA requirements and processes by:

(a) Developing a PIA template and instructions on how to complete it;

(b) Providing guidance and assistance on meeting OMB and VA requirements;

(c) Reviewing and analyzing each PIA, so that a recommendation for approval can be made to the CIO;

(d) Submitting completed PIAs to OMB, as appropriate; and

(e) Publishing approved PIAs on the appropriate VA Web site.

(2) **Director, Records Management Service**. The Director shall:

(a) Review Joint Information Collection Request (ICR) and the associated PIA for new electronic information collections, as part of the OMB 83-1 (SF83), Paperwork Reduction Act Submission, Supporting Statement, to ensure that the information is addressed and identified within the structure of the Supporting Statement to the ICR;

(b) Coordinate with Privacy Service when amending an ICR to collect information that is significantly different in character from the original collection;

(c) Submit the Joint ICR and PIA to OMB, and make it publicly available under the mandates of the Paperwork Reduction Act; and

(d) Review Systems of Records (SOR) notices.

b. **Inspector General.** This Office will be requested to:

(1) Provide assistance and guidance to the Privacy Service on the oversight and design of PIAs; and

(2) Provide recommendations on VA PIA compliance.

c. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials shall:

(1) Ensure that IT Project Managers submit timely and accurate PIAs;

(2) Ensure that PIAs are submitted in parallel with the Exhibit 300;

(3) Work with the Privacy Service to finalize each PIA; and

(4) Monitor compliance with security and privacy provisions in each PIA for each IT system under their authority.

d. **Project Managers (PM).** PMs shall:

(1) Determine whether a PIA is necessary for their IT project;

(2) Complete an initial PIA in a timely and accurate manner in accordance with the guidance established by the Privacy Service;

(3) Update PIAs annually; and

(4) Ensure that each IT system is compliant with the security and privacy requirements described in each PIA.

3. **ESSENTIAL REQUIREMENTS AND PROCEDURES.** VA requires that PIAs be updated and completed in parallel with the VA IT investments described in related Exhibit 300s. OMB Memo 03-22 mandates that PIAs are to be used to assess whether PPI is handled in conformance with applicable legal, regulatory, and privacy policy requirements. PIAs shall be used to determine the risks and effects of collecting, maintaining, and disseminating electronic information in identifiable form, and the protections and alternative processes for handling this information to mitigate potential privacy risks. The following are required elements of the PIAs:

a. The VA Privacy Service shall provide guidance and requirements for the completion of the PIA. VA requires that PIAs shall be completed for VA IT systems that collect, maintain, or disseminate information of the public totaling at least ten individuals. PIAs shall be conducted before:

(1) Developing or procuring IT systems that collect, maintain or disseminate information in identifiable form from or about members of the public, and shall address:

(a) Statement of need;

(b) Functional requirements;

(c) Analysis of feasibility, cost benefits and alternatives;

(d) An initial risk assessment; and

(e) The impact the system will have on an individual's privacy.

(2) Initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, VA personnel or other authorized users); or

(3) Deploying a new system that contains privacy elements not addressed in the PIA written at the concept phase.

b. The PIA form, available in the Capital Asset Management System (CAMS), must be completed for all VA projects with IT systems that maintain personal information on the public;

c. PIAs shall be completed in parallel with the investment's related Exhibit 300, to be subject to, and followed by:

(1) Approval by the CIO;

(2) Submission to the OMB Office of Electronic Government; and

(3) Publication on the VA Internet Web site except in circumstances of:

(a) National security (classified information);

(b) Damage to law enforcement processes; or

(c) Competitive business interest.

d. PIAs shall not include information in identifiable form;

e. The scope and content of the PIA shall be commensurate with the size and complexity of the IT system so that major information systems shall have a more extensive analysis of:

(1) The consequences of collection and flow of information;

(2) The alternatives to established methods for the collection and handling of information;

(3) The appropriate measures to mitigate risks for each alternative; and

(4) The rationale for the final design choice or business process.

f. Simple database systems which involve routine information, and limited use and access shall use a standardized template provided by the Privacy Service (see Appendix A).

g. PIAs shall be performed and updated as necessary when a system change is made, to determine if a privacy risk has been created by the change such as when:

(1) Paper records are converted to electronic records;

(2) There are changed information collection authorities or business processes;

(3) Information is changed from anonymous to identifiable;

(4) New technologies are applied to the system that significantly change the way identifiable information is managed creating new access and vulnerability concerns;

(5) Changes in business processes that cause systems to be merged, centralized or matched to other systems create new use, disclosure, access, and vulnerability concerns;

(6) VA obtains identifiable information from other sources; and

(7) There are significant uses and sharing of data with another Federal agency. In such cases the lead agency shall prepare the PIA.

h. No PIA is required when a system has been assessed in an evaluation similar to a PIA (such as an SOR) when privacy issues are unchanged, or when information relates to internal government operations;

i. The process of performing a PIA will also identify the choices made regarding the design or selection of an IT system; and

j. When conducting a PIA, the life cycle of the information (collection, use, retention, processing, disclosure and destruction) and how each stage of the life cycle may affect the privacy of the individually identifiable information must be evaluated.

4. ESSENTIAL ELEMENTS OF THE PIA

OMB Memo M-03-22 requires that PIAs have the following required minimal content:

a. What information is to be collected, (e.g., the nature and source);

b. Why the information is being collected (e.g., to determine eligibility);

c. The intended uses of the information (e.g., to verify existing data);

d. With whom the information will be shared (e.g., another agency for a specified programmatic purpose);

e. What opportunities individuals have to decline to provide (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than the required or authorized uses), and how individuals can grant consent;

f. How the information will be secured (e.g., administrative and technological controls); and

g. Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

5. RELATIONSHIP REQUIREMENTS TO OTHER LAWS. All PMs must update their PIAs annually. Under guidelines established by the Privacy Service, and in accordance with Federal law and guidance, PIAs may be performed and submitted to OMB through the Privacy Service, under the provisions of the Paperwork Reduction Act (PRA) and the Privacy Act as described below:

a. **Paperwork Reduction Act (PRA)**. Under the Privacy Service guidelines, VA may perform and submit PIAs to OMB and make them publicly available as part of the SF 83, Supporting Statement, as Joint Information Collection Requests (ICR). Program managers shall comply with the requirements for such submissions as provided by the Privacy Service.

b. **Privacy Act of 1974**. Under the Privacy Service guidelines VA may:

(1) Conduct a PIA when developing a Systems of Record (SOR) notice for an IT system where the PIA and SOR overlap;

(2) Make a PIA publicly available in the Federal Register as part of a Privacy Act SOR notice for an IT system; and

(3) Assess the need for a PIA in consultation with the Privacy Service, when changes to an SOR notice for an IT system are issued.

6. REFERENCES

a. Clinger-Cohen Act of 1996, 40 U.S.C. 11101 and 11103.

b. E-Government Act of 2002 (Pub. L. 107-347), 44 U.S.C. 36.

c. Freedom of Information Act (FOIA), 5 U.S.C. 552.

d. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

e. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.

f. OMB Memo-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

g. Paperwork Reduction Act, 44 U.S.C. 35, and 5 C.F.R. Part 1320.8.

h. Privacy Act of 1974, 5 U.S.C. 552a.

i. VA Directive and Handbook 6210, Automated Information Systems Security.

j. VA Directive 6212, Security of External Electronic Connections.

k. VA Directive 6214, Information Technology Security Certification and Accreditation Program.

l. VA Handbook 6300.2, Management of the Vital Records Program.

m. VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act (FOIA).

n. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA).

o. VA Handbook 6300.5, Procedures for Establishing and Managing a Privacy Act System of Records.

7. DEFINITIONS

a. Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.

b. Information Technology (IT). In accordance with the definition in the Clinger-Cohen Act, IT is defined as 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.

c. Major Information System. A large and sensitive system or project that requires special management attention because of its importance to the mission of VA; high development, operating and maintenance costs; high risk or return; or significant role in the administration of VA programs, finances, property or other resources.

d. Privacy Impact Assessment (PIA). An analysis, required by the E-Government Act of 2002, of how VA electronic personal information is maintained, used, and collected.

e. Privacy-Protected Information (PPI). Electronic information in a VA IT system that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which VA intends to identify specific individuals in conjunction with other data elements.

PRIVACY IMPACT ASSESSMENT TEMPLATE

Questions: The following is a sample template of questions to be presented in the Capital Asset Management System (CAMS), answered from a drop down menu or by a narrative description by all Project Managers of systems that maintain personally identifiable information on the public totaling at least 10 individuals. Several of the questions in the template require narrative descriptions in addition to the drop down menu choices.

1. What personally identifying information is collected?

a. What are the sources of the information?

b. What are the media used to collect the information? (Provide a description of the collection media.)

2. Why is the information collected? (Provide a concise description of the reason for collecting the information, e.g., eligibility determination.)

3. What is the intended use of the information? (Provide a description of the common uses of the information, e.g., providing benefits or healthcare.)

4. With whom will the information be shared? (Provide a description that includes the names and entities with whom the information will be shared, as well as any sharing agreements.)

5. How will individuals consent for collection and use of their personal information? (Describe the methods used to provide consent to collect the information.)

6. How will the information be secured? (Describe the system's security, e.g., administrative and technological controls.)

7. Is this system or collection part of a Privacy Act System of Records (SOR)? (Provide the SOR number, if known, and a description of the system as a Privacy Act SOR.)

8. Identify what choices were made regarding an IT system or collection of information as a result of performing the PIA. (Describe the choices made from the drop down menu.)