

PRIVACY IMPACT ASSESSMENT (PIA)

- 1. REASON FOR ISSUE:** This handbook establishes Department-wide procedures for conducting Privacy Impact Assessments (PIA), and implements the policies pertaining to PIAs that are set forth in Department of Veterans Affairs (VA) Directive 6502, VA Enterprise 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 VA 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 completion and submission of PIAs.
- 3. RESPONSIBLE OFFICE:** Office of the Assistant Secretary for Information and Technology (005), Office of Information Protection and Risk Management (005R), Office of Privacy and Records Management (005R1), VA Privacy Service (005R1A).
- 4. RELATED DIRECTIVE:** VA Directive 6502, VA Enterprise Privacy Program; VA Directive 6508, Privacy Impact Assessments (PIAs).
- 5. RESCISSIONS:** VA Handbook 6502.2, Privacy Impact Assessment, October 21, 2004.

CERTIFIED BY:

/s/
Roger W. Baker
Assistant Secretary for
Information and Technology

**BY DIRECTION OF THE SECRETARY OF
VETERANS AFFAIRS:**

/s/
Roger W. Baker
Assistant Secretary for
Information and Technology

Distribution: Electronic

PRIVACY IMPACT ASSESSMENT (PIA)

CONTENTS

PARAGRAPH	PAGE
1. PURPOSE AND SCOPE	5
2. RESPONSIBILITIES.....	6
3. PREREQUISITES, PROCEDURES, FREQUENCY AND TIMELINESS.....	10
4. OTHER REQUIRED USES OF PIAs.....	13
5. RELATIONSHIP REQUIREMENTS TO OTHER LAWS.....	13
6. REFERENCES	14
7. DEFINITIONS.....	14

PRIVACY IMPACT ASSESSMENT (PIA)

1. PURPOSE AND SCOPE

a. This handbook provides the procedures and requirements for conducting Privacy Impact Assessments (PIA). The Department of Veterans Affairs (VA or Department) is required to perform PIAs in accordance with the privacy provisions of the E-Government Act of 2002 (Act), Office of Management and Budget (OMB) M-03-22, VA Directive 6502, VA Enterprise Privacy Program, paragraph 2.d., and VA Directive 6508, Privacy Impact Assessments.

b. The purpose of the Act 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 privacy provisions of the Act and implementing OMB M-03-22 require Federal agencies to conduct privacy assessments with regard to the personally-identifiable information (PII) they collect, use, maintain, and distribute in information technology (IT) systems.

c. VA is required by OMB to assess how it manages PII throughout the information life cycle. The PIA is the compliance initiative designed to meet this requirement. The VA Privacy Service establishes VA requirements and guidance on the development, completion, and periodicity of PIAs.

d. The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

e. The PIA informs VA's senior leadership and program offices in their deliberations about how to implement privacy protections into new and existing programs. Senior leadership and Program Managers have the overall responsibility and commitment of ensuring that all VA programs respect and protect PII, but these senior leaders and Program Managers may not have the privacy expertise necessary to evaluate how best to do so. The PIA helps them identify the privacy issues and evaluate whether activities have adequately addressed them.

f. Section 208 of the Act requires Federal agencies to complete PIAs prior to: (1) developing or procuring information technologies that collect, maintain, or disseminate PII; or (2) initiating, consistent with the Paperwork Reduction Act, a new collection of PII from ten or more individuals in the public. The Act does not require that PIAs be conducted on systems that collect information solely about Federal employees. Nevertheless, VA considers the protection of employees' PII to be just as important as the PII of the public. By failing to properly protect employees' PII, the confidence of the public in VA's ability to protect the public's PII is

compromised. Therefore, the VA Privacy Service conducts PIAs on all systems that collect, maintain or disseminate the PII of any VA employee or contractor. The VA Privacy Service has developed the PIA to help identify when an IT system collects or uses PII. By completing the Tab 2 "System Identification" the questions are designed to determine if a full PIA is required due to the presence of PII or if just completing this tab is sufficient. VA Privacy Service requires every IT system to have a completed PIA as part of the Certification and Accreditation (C&A) process.

g. This handbook delineates responsibilities, and discusses prerequisites and procedures for conducting PIAs.

2. RESPONSIBILITIES

a. **The Assistant Secretary for Information and Technology (AS/IT).** The AS/IT, as the Department's Chief Information Officer (CIO), shall:

(1) Ensure that a mechanism is in place for the review and approval of all PIAs and Exhibit 300s, per OMB's instructions;

(2) Ensure the monitoring of all VA-wide IT systems for compliance with the security and privacy statements found in the PIAs of said IT systems;

(3) Submit all approved PIAs to OMB; and

(4) Designate the Associate Deputy Assistant Secretary (ADAS) for Privacy and Records Management as the principal Department official responsible for ensuring the reporting of all PIAs received.

b. **Deputy Assistant Secretary (DAS), Office of Information Protection and Risk Management.** The DAS shall:

(1) Perform all PIA duties and responsibilities as designated by the AS/IT;

(2) Ensure that PIAs are performed as a part of the C&A and OMB Exhibit 300 processes; and

(3) Ensure that completed PIAs are submitted to the AS/IT.

c. **Associate Deputy Assistant Secretary (ADAS), Office of Privacy and Records Management.** The ADAS shall:

(1) Perform all PIA duties and responsibilities as designated by the DAS;

(2) Ensure that a PIA template and instructions for completion of PIAs are made available to System Owners (SO);

(3) Ensure that guidance and assistance about the PIA process is provided to parties responsible for the completion of PIAs;

(4) Ensure that all completed PIAs are submitted to the Department CIO; and

(5) Ensure that PIAs are published appropriately.

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

(1) Performing all PIA duties and responsibilities as designated by the ADAS, Office of Privacy and Records Management;

(2) Developing a template and instructions on how to complete PIAs;

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

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

(5) Submitting completed PIAs to the VA CIO, as appropriate; and

(6) Publishing approved PIAs on the appropriate VA Website.

e. **Director, Enterprise Records Service.** The Director shall:

(1) Review Joint Information Collection Requests (ICR) and associated PIAs 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;

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

(3) Submit the ICR and PIA to the VA CIO, and make it publicly available under the mandates of the Paperwork Reduction Act; and

(4) Conduct periodic reviews of Systems of Records Notices (SORN).

f. **Inspector General.** This office will be requested to:

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

(2) Provide recommendations on VA PIA compliance.

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

- (1) Ensure that Program Managers and Project Managers (PM) submit timely and accurate PIAs;
- (2) Ensure that PIAs are submitted in parallel with the appropriate OMB Exhibit 300 documentation;
- (3) Work with the VA Privacy Service to finalize each PIA; and
- (4) Monitor compliance with security and privacy provisions in each PIA for each system, program and project under their authority.

h. **Program Managers.** Program Managers shall:

- (1) Work with PMs and SOs to ensure that PIAs associated with their projects and systems within their programs are complete and accurate;
- (2) Provide the information necessary for completion of the PIA to their SOs, Privacy Officers (PO), and Information Security Officers (ISO);
- (3) Ensure that PIAs are completed in a timely and accurate manner in accordance with the guidance provided by the VA Privacy Service;
- (4) Ensure that PIAs for projects for which they are responsible are updated annually; and
- (5) Ensure that each project for which they are responsible is compliant with the security and privacy requirements described in each PIA.

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

- (1) Work with appropriate Program Managers, ISO, PO, and SOs to ensure that PIAs associated with their projects are complete and accurate in accordance with the guidance provided by the VA Privacy Service;
- (2) Complete and submit initial PIAs during the development or procurement phase of a new technology or system that will handle or collect PII;
- (3) Update PIAs when major changes take place or provide a Validation Letter annually;
- (4) Update all PIAs every 3 years; and
- (5) Ensure that each project or system for which they are responsible is compliant with the security and privacy requirements described in its PIA.

j. **System Owner (SO).** The SOs shall:

- (1) Work with the Program Managers, PMs, appropriate ISOs, POs, and System Developers/Designers to address the system's privacy issues that are revealed by completing a PIA;
- (2) Work with PMs in the preparation of PIAs;
- (3) Obtain Program Managers' and PMs' approval of the PIA report;
- (4) Submit PIAs to the VA Privacy Service for review and approval; and
- (5) Serve as the point of contact for the system.

k. **System Developers/Designers.** System Developers/Designers shall:

- (1) Ensure that system design and specifications conform to legal, regulatory and policy standards for privacy and security; and
- (2) Ensure that proper technical controls are in place for safeguarding PII from unauthorized access.

l. **Data Owners.** Data Owners shall:

- (1) Work with Program Managers, PMs, SOs, ISO, POs and System Developers to ensure that appropriate privacy protections are in place;
- (2) Serve as the point of contact for questions related to system data; and
- (3) Respond to questions from Program Managers, ISOs, PMs, SOs, or System Developers related to the PIA submission.

m. **Privacy Officers.** POs shall provide assistance to SOs, PMs, and the VA Privacy Service in developing PIAs and ensure that all questions are fully and accurately answered and of a quality that will ensure approval by the VA Privacy Service. POs shall also coordinate with the VA Privacy Service to finalize each PIA. In addition, POs will coordinate with their local ISOs to ensure that foreseeable privacy risks have been identified and documented in all PIA submissions.

n. **Information Security Officer.** ISOs shall maintain read-write access to the PIA module found in the Security Management and Reporting Tool (SMART).

3. PREREQUISITES, PROCEDURES, FREQUENCY AND TIMELINESS

a. Prerequisites.

(1) The responsible persons shall conduct a full PIA before:

(a) Developing or procuring a new IT system, program, project or practice which will collect, use, maintain or distribute PII;

(b) Initiating a new electronic collection of PII about ten (10) or more individuals;

(c) Issuing a new VA rulemaking which will result, or is likely to result in, collection of PII; and

(d) Modifying an IT system, program, project or practice where the modification may create a major change. Major changes include, but are not limited to:

1. Converting paper-based records to electronic systems;

2. Applying functions to an existing information collection to change anonymous information into information in identifiable form (IIF);

3. Creating new uses of an existing IT system, program, project or practice, including application of new technologies, which significantly change how IIF is managed;

4. Adopting or altering Practices so that government databases holding PII are merged, centralized or matched with other databases, or are otherwise significantly manipulated;

5. Applying user-authenticating technology (e.g., password, digital certificate, biometric) for the first time;

6. Purchasing or obtaining PII from commercial or public sources and systematically incorporating it into existing IT systems, programs and projects (merely querying such a source on an ad hoc basis using existing technology does **not** trigger the PIA requirement);

7. Working with another agency on shared functions involving significant new uses or exchanges of PII, such as cross-cutting E-Government initiatives (in such cases, VA is only required to prepare a PIA if it is acting as the lead agency for the initiative);

8. Altering business process results in significant new uses or disclosures of information, or incorporation into the system of additional items of PII; or

9. Adding PII to a collection when the addition of the PII raises the risks to personal privacy (for example, the addition of health or financial information).

(2) A PIA must be completed and submitted for every system, program, project, practice or rulemaking. Completion of only Section 1 "System Identification" under Tab 2 is considered a "partial PIA," and may be submitted when:

(a) A government-run Website, IT system, program, project, practice or other collection of information does not collect, use, maintain or distribute PII;

(b) A government-run public Website where the user is given the option of contacting the site operator for the limited purpose of asking questions or providing comments;

(c) The system is a national security system;

(d) All elements of a PIA are addressed in a data matching or comparison agreement governed by the computer matching provisions of the Privacy Act of 1974;

(e) All elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the Act ;

(f) Developing IT systems, programs, projects, practices or rulemakings, or collecting non-identifiable information, for a discrete purpose that does not involve matching with or retrieval from other databases that generate PII or business identifiable information; or

(g) Minor changes are made to an IT system, program, project, practice or rulemaking, or other collections that do not create new privacy risks.

(3) In lieu of a new PIA being submitted, a PIA Validation letter may be submitted as an addendum to the PIA on file under the following circumstances:

(a) The system has not been identified by the VA Privacy Service as being due for a new PIA under its triennial review schedule;

(b) No major change, as defined by this handbook, have taken place;

(c) No new PIA is necessary based upon any changes made;

(d) All information privacy and security policies, guidelines and procedures have been followed and are being enforced;

(e) A list of changes is included with the Validation Letter that documents that, if any change has occurred, no security or privacy control has been altered; and

(f) The Validation Letter is signed by the SO, the PO, the CIO and the ISO.

b. Procedures.

(1) When any of the circumstances described in Section 3.a.(1) exist, the responsible party shall conduct, complete, and submit the PIA.

(2) For all PIAs, the template is found on either:

(a) The Information Protection Portal until such time as an electronic form is developed for the submission of PIAs at <http://vawww.privacy.va.gov/PIA.asp>; or

(b) The PIA module found in the SMART database.

(3) The SO shall submit the completed PIA to the VA Privacy Service:

(a) In hard copy, addressed to Department of Veterans Affairs, 810 Vermont Avenue, Washington, DC 20420, Attn: VA Privacy Service, or

(b) Electronically at privacyservice@va.gov. Please note that PIAs containing VA sensitive data as defined in VA Handbook 6500 that are submitted via email must be submitted in encrypted form.

(4) The VA Privacy Service is responsible for reviewing and approving completed PIAs. During the review, the VA Privacy Service will examine whether privacy risks are identified and addressed. The VA Privacy Service will also assess the PIA content for conformity with privacy, legal and regulatory requirements.

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

(6) The VA Privacy Service will post all approved PIAs on the VA Privacy Portal at http://www.privacy.va.gov/Privacy_Impact_Assessment.asp.

c. Frequency.

(1) An initial PIA shall be conducted, and a completed PIA shall be submitted to the VA Privacy Service as described in Section 3. a. and b. above.

(2) Thereafter, the responsible party shall, on an annual basis:

(a) Submit a Validation Letter under the process described above, in the format provided by the VA Privacy Service, certifying that there have been no major changes to the IT system, program, project or practice; or

(b) Submit a new PIA.

(3) Not less than triennially, the responsible party shall submit a new PIA.

d. **Timeliness.** A PIA or Validation Letter shall be submitted to the VA Privacy Office no later than the date determined.

4. OTHER REQUIRED USES OF PIAs

a. **C&A Process.** Responsible parties for all IT systems, programs, projects and practices must conduct and submit a completed PIA template as a part of the C&A process. PIAs must be completed as a part of the C&A process.

b. **OMB Exhibit 300's.**

(1) The responsible party for each VA IT system that collects, uses, maintains or distributes PII must also include a completed PIA template with the system's OMB Exhibit 300.

(2) More than one system, program, project, or practice may be "rolled up" into a larger program for each OMB Exhibit 300 completed. In this instance a PIA will **not** be completed using the template located in the SMART database, but must be completed and submitted to the VA Privacy Service using the template that is available at the VA Information Protection Portal located at: <https://vaww.infoprotection.va.gov>.

c. **Submittal of PIAs.** In each instance, the completed PIA template shall be submitted to the VA Privacy Service using one of the methods described in Section 3.b.(2).

5. RELATIONSHIP REQUIREMENTS TO OTHER LAWS

In accordance with Federal law and guidance, PIAs may be performed and submitted to OMB through the VA Privacy Service, under the provisions of the Paperwork Reduction Act and the Privacy Act of 1974 as described below:

a. **Paperwork Reduction Act.** Under the VA Privacy Service guidelines, VA may perform and submit PIAs to OMB and make them publicly available as part of the Standard Form (SF) 83, Supporting Statement, as ICRs. Responsible Persons shall comply with the requirements for such submissions as provided by the VA Privacy Service.

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

(1) Conduct a PIA when developing a SORN for an IT system where the PIA and system of records overlap;

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

(3) Assess the need for a PIA in consultation with the VA Privacy Service, when changes to an SORN 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. Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, *et seq.*
- d. Freedom of Information Act (FOIA), 5 U.S.C. 552.
- e. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.
- f. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.
- g. OMB Memo-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
- h. Paperwork Reduction Act, 44 U.S.C. 35, and 5 C.F.R. Part 1320.8.
- i. Privacy Act of 1974, 5 U.S.C. 552a.
- j. VA Handbook 6300.2, Management of the Vital Records Program.
- k. VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act (FOIA).
- l. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA).
- m. VA Handbook 6300.5, Procedures for Establishing and Managing a Privacy Act System of Records.
- n. VA Directive and Handbook 6500, Information Security Program.

7. DEFINITIONS

- a. **Data Owner.** A person who can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.
- b. **Individual.** Any citizen of the United States or alien lawfully admitted for permanent residence.
- c. **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.

d. **IT System.** Any series or grouping of equipment, software or interconnected systems or subsystems used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

e. **Major Change.** A change to the information collected or maintained that could result in greater disclosure of information or a change in the way personal data is used.

f. **Personally-Identifiable Information (PII).** For purposes of this VA Privacy Service Handbook, PII shall be a subcategory of VA sensitive information/data as defined by VA Handbook 6500. PII is any information about an individual that can reasonably be used to identify that individual that is maintained by VA, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, etc., including any other personal information which is linked or linkable to an individual.

g. **Practice.** Actual performance or application of a repeated or customary action.

h. **Program.** A coordinated group of projects, often for a specific purpose, that are managed in a coordinated way. Programs usually include an element of ongoing work.

i. **Project.** A temporary endeavor consists of several tasks undertaken to create a unique product, service, or result. An IT project may consist of tasks affecting one or more IT systems.

j. **Record.** Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

k. **Responsible Party.** Those required to account for the performance or content of IT systems or data collections. Examples include: SOs, Data Owners, Program Managers and PMs.

l. **Rulemaking.** The process that executive agencies use to implement interpret or prescribe law or policy, or to describe the organization, procedure or practice requirements of any agency. The term includes the amendment or repeal of an existing rule or regulation.

m. **System.** A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

n. **System Owner.** An administrator of distributed or central computer systems who is responsible for system storage management, fault management, configuration management, performance management, and user activities monitoring.

o. **Validation Letter.** A letter from a responsible party that validates the current state of the IT asset stating that that no change has occurred which requires a new PIA. This letter is appropriate for those years when a PIA is not needed.