Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6508.1
Transmittal Sheet
July 30, 2015

PROCEDURES FOR PRIVACY THRESHOLD ANALYSIS AND PRIVACY IMPACT ASSESSMENT

I. REASON FOR ISSUE: To establish the process and procedures for VA Directive 6508, Implementation of the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA). This handbook, sets forth the methodology by which the VA will incorporate the PTA, as recommended by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), into the required risk-based compliance process of the PIA pursuant to the E-Government Act of 2002 (Pub. L. 107-347).

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This handbook:

a. Establishes new processes, procedures, and responsibilities for reviewing and assessing the privacy implications of information maintained in VA information technology (IT) systems, rule makings, programs, and/or projects through the inclusion of the PTA;

b. Institutes new VA responsibilities, processes, and procedures for completion and submission of the PTA; and

c. Reestablishes VA responsibilities, processes, and procedures for completion and submission of the PIA.

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, Privacy Service (005R1A).

4. RELATED DIRECTIVE/HANDBOOK: VA Directive 6502, Enterprise-Wide VA Privacy Program; VA Directive 6508, The Implementation of the Privacy Threshold Analysis and the Privacy Impact Assessment.

5. RESCISSION: VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment, November 16, 2010

CERTIFIED BY:	**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:**
/s/ LaVerne H. Council Assistant Secretary for Information and Technology	***/s/*** LaVerne H. Council Assistant Secretary for Information and Technology

IMPLEMENTATION OF PRIVACY THRESHOLD ANALYSIS AND PRIVACY IMPACT ASSESSMENT

TABLE OF CONTENTS

IMPLEMENTATION OF PRIVACY THRESHOLD ANALYSIS AND PRIVACY IMPACT ASSESSMENT

1. PURPOSE AND SCOPE

This handbook establishes a detailed methodology for the inclusion of the PTA into the VA enterprise-wide privacy compliance process. In addition, this policy discusses the processes and procedures for the PIA. The PTA is a privacy compliance and risk management tool instrumental in determining whether Personally Identifiable Information (PII) and/or Personal Health Information (PHI) is being collected and maintained by an Information Technology (IT) System, rulemaking, program, and/or project. The PTA facilitates the creation of a privacy risk assessment portfolio maintained by the VA Privacy Service. The PTA and PIA embody the required collaboration of officials in VA programmatic offices, identified in the policy; Information Security Officers (ISO); Privacy Officers (PO); System Managers/System Owners and the VA Privacy Service.

PII and PHI are subsets of Sensitive Personal Information (SPI). The term SPI will be used to describe both throughout the policy.

2. PTA AND PIA GENERAL REQUIREMENTS

a. PTA:

(1) The PTA is a privacy compliance and risk management assessment tool designed to:

(a) Document the collection, creation, maintenance, use and/or disclosure of SPI collected within a VA IT system, program, rulemaking, and/or project, which will result, or is likely to result in the collection of SPI.

(b) Determine if additional privacy requirements such as a PIA and System of Records Notice (SORN) is needed.

(2) As identified in VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, there are two types of PTAs further discussed in the policy:

(a) Program Management Accountability System (PMAS) PTA Template *NOTE: Standard Template is found on the Privacy Service Intranet.*; and

(b) The Standard PTA Template. *NOTE: Standard Template is found on the Privacy Service Intranet.*

(3) PTAs are reviewed and certified annually.

(4) PTAs are incorporated in the Authorization and Accreditation (A&A) process when it has been determined that SPI is not collected.

b. PIA:

(1) PIA is designed to identify the privacy and security risks associated with the use of SPI by a program, project, IT system or rulemaking

(2) The PIA ensures the use of privacy protections compatible with the identified risks throughout all phases of the System Development Life Cycle (SDLC) of IT systems. VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning.

(3) Pursuant to Title III section 208 of the E-Government Act of 2002, The Federal Information Security Management Act of 2002 (FISMA) and Office of Management and Budget (OMB) Guidance M-03-22, Implementing the Privacy Provisions of the E-Government Act of 2002, VA will:

(a) Conduct PIAs for electronic information systems and collections for all new and substantially changed (IT) systems, rulemakings, programs, and/or projects that have been determined by the adjudication of the PTA.

1. Publish PIAs on the VA Privacy Service website to facilitate transparency;

2. Report annually to OMB on compliance with FISMA requirements; and

(b) PIA is incorporated in the A&A process as an element in identifying privacy risks and proper level of security within an IT system.

3. APPLICATION OF THE PTA

a. **PMAS PTA:** The PMAS PTA is required as a part of the reviews described in VA Directive 6071, Project Management Accountability System (PMAS), Milestone 0 and Milestone 1.

(1) The PMAS Project Manager, is responsible for coordinating the completion of the PMAS PTA with other relevant Integrated Project Team (IPT) members before the PMAS active state of the IT project development.

(2) As part of the IPT, a PO is assigned by the Business Sponsor; and

(3) The completed PMAS PTA will identify the collection and maintenance of SPI by the program, project and/or IT system. If it is determined that SPI is collected, a PIA is required

b. **Standard PTA** : The purpose of the Standard PTA is to identify programs, projects and IT systems that collect and maintain SPI. It is required for efforts associated with FISMA compliance and to incorporate into the A&A package. A Standard PTA will be completed upon:

(1) Development or procurement of any IT system that will handle or collect SPI and document major changes to existing IT systems with already existing PIAs;

(2) Creation of new forms or other collections of SPI (including but not limited to collections that trigger the Paperwork Reduction Act); and

(3) Issuance of new or updated rulemaking and IT systems that involve the collection, use, and maintenance of SPI;

4. APPLICATION OF THE PIA

a. Administrations and staff offices are required to complete a PIA when:

(1) It has been identified by a PTA that an IT system, program, and/or a project collects SPI;

(2) Developing, procuring IT systems, or projects that collect, maintain or disseminate information in identifiable form from or about member of the public

(3) Initiating a new electronic collection of information in identifiable form for ten (10) or more persons;

(4) A major change occurs to an IT system. Major changes include, but are not limited to**:**

(a) **Conversions** – Converting paper-based records to electronic systems.

(b) **Anonymous to Non-anonymous** - Applying functions to an existing information collection to change anonymous information into information in identifiable form (IIF);

(c) **Significant System Management Changes** – Creating new uses of an existing IT system, program, project or practice, including application of new technologies which significantly change how IIF is managed;

(d) **Significant Merging** – Adopting or altering practices so that government databases holding SPI are merged, centralized or matched with other databases or are otherwise significantly manipulated;

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

(f) **Commercial Sources** – Purchasing or obtaining SPI 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);

(g) **New Interagency Uses** – Working with another agency on shared functions involving significant new uses or exchanges of SPI, 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);

(h) **Internal Flow or Collection** – Altering a business process results in significant new uses or disclosures of information or incorporation of additional SPI into the system; or

(i) **Alteration in the Character of Data** – Adding SPI to a collection when the addition of the SPI raises the risks to personal privacy (for example, the addition of health or financial information).

(j) **Important Note:** IT systems that require a PIA may also require a SORN. For more information on SORN requirements and process, contact the Privacy Service at 202-273-5070 or via email at privacyservice@va.gov. You can also consult VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records.

b. If there are no changes with the existing PIAs, administrations and staff offices are required to review and update their PIAs every three years.

5. PROCEDURAL SUBMISSION REQUIREMENTS

a. PTA:

(1) The PO will:

(a) Conduct the PTA by following the guidance and directions in the *Privacy and Records Management, Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) Supplemental* guidance located on the Privacy Service Intranet.

(b) Complete the PTA in its entirety and submit it to the Privacy Service for an initial review

(2) The Privacy Service will:

(a) **If the PTA determines that there is no PII collected:**

1. The System Owner/System Manager, PO, and ISO will be notified that no further action is needed;

2. A copy of the PTA will be provided to the System Owner/System Manager, PO, and ISO as privacy compliance and risk management documentation indicating an IT system has been assessed for privacy implications and is accepted to include into the A&A process; and

(b) **If the PTA indicates that PII is being collected**: A copy of the PTA will be provided to the SO, PO and ISO as privacy compliance and risk management documentation indicating an IT system has been assessed for privacy implications and a PIA is required.

b. PIA:

(1) The PO will:

(a) Coordinate with their local ISOs and System Managers Privacy Service to ensure that all data and associated risks are identified and documented in the PIA submissions.

(b) Work with their ISOs and System Managers to ensure the PIA(s) for each IT system, program, project, and/or rulemaking is completed in full and is of a quality that will reasonably ensure approval by Privacy Service PIA Support Team.

(2) The Privacy Service PIA Support Team will: Provide the System Owner/System Manager, PO and ISO access the PIA template in located in the *Privacy and Records Management, Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) Supplemental* Guide Privacy Service Intranet.

(a) Review the draft PIA and coordinate changes with the PO as necessary;

(b) Ensure electronic signatures of the PO, ISO, and SO are present;

(c) Send PIA to the Chief Information Officer (CIO) for review and signature. Once the CIO reviews and signs the PIA, it is officially approved and completed.

(d) Notify the SO, PO and ISO of the approval and approved PIA is incorporated into the IT system's A&A package by the ISO;

(e) Post approved PIAs to the Privacy Service PIA Internet site.

c. PTA AND PIA: The Privacy Service will:

(1) Monitor completion dates of Standard PTAs and PIAs and administer requirements of development and completion in accordance with NIST SP-800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), and E-Government Act of 2002, Title III, FISMA.

(2) Review Standard PTAs and PIAs on projects, programs and IT systems that collect, maintain or disseminate the SPI of any employee or contractor.

6. RESPONSIBILITIES.

a. **Assistant Secretary for Information and Technology (ASIT).** ASIT, as the Department's CIO and Senior Agency Official for Privacy (SAOP), will:

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

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

(3) Designate the Director, Office of Privacy and Records Management (OPRM) as the principal Department official responsible for ensuring the reporting of all PIAs received pursuant to the E-Government Act of 2002.

b. **The Director, OPRM.** The Director, OPRM will:

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

(2) Ensure that the PTA and PIA templates and instructions are made available to the PO, SO and ISO; and

(3) Ensure that guidance and assistance is provided that meets OMB and VA requirements;

c. **Director, Privacy Service.** The Director will establish Enterprise-wide privacy compliance requirements and processes by:

(1) Enforcing all PTA and PIA compliance responsibilities as designated by the Director OPRM

(2) Developing PTA and PIA templates and instructions;

(3) Ensuring that guidance and assistance is provided in compliance with the E-Government Act of 2002; prescribed NIST standards, and other VA policies;

(4) Reviewing each PIA received and submitting adjudicated PIAs to the O&IT CIO, as appropriate; and

(5) Publishing approved PIAs on the Privacy Service web site located at http://www.oprm.va.gov/privacy/pia.aspx.

d. **Director, Records Management Service.** The Director will:

(1) Perform PIA related duties and responsibilities as designated by the Director, OPRM; and

(2) Review Information Collection Requests (ICR) to determine whether the information requested contains privacy sensitive information that could potentially require a PIA.

e. **Inspector General.** This Office will be requested to independently create and maintain PTAs, PIAs, SORNs, and similar documentation as part of its self-governing IT and privacy operations.

f. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials will be requested to:

(1) Work in conjunction with the Privacy Service to enforce PTA and PIA requirements; and

(2) Monitor compliance with security and privacy statements in each PIA for all rulemaking, IT programs, and/or pilot projects under their authority.

g. **Program Managers.** Program Managers will:

(1) Work with Project Managers, System Managers/System Owners, POs, and ISO to complete the PTA and determine whether a PIA is necessary for the rulemaking, IT programs, and/or pilot projects being commenced or significantly modified;

(2) Validate that PTAs and PIAs are completed in a timely and accurate manner in accordance with guidance established by this Directive;

(3) Ensure that PTAs are reviewed annually and PIAs are updated accordingly; and

(4) Affirm that each project for which they are responsible is compliant with the security and privacy mitigations stated in the PIA.

h. **Project Managers.** Project Managers will:

(1) Coordinate with POs, Program Managers, ISOs, and System Managers/System Owners to complete the PTA and complete a PIA, if necessary;

(2) Ensure that PTAs and PIAs are completed in a timely and accurate manner in accordance with the guidance established by this Directive;

(3) Coordinate with their POs, ISOs, System Managers/System Owners, and with the Privacy Service to ensure that all PTAs and PIAs under the responsibility of these officials are finalized;

(4) Initiate or update all PTAs and PIAs as set forth in this policy; and

(5) Ensure that each rulemaking, IT program, and/or pilot project is compliant with security and privacy requirements described in each PIA.

i. **System Managers/System Owners.** The System Manager/System Owners will:

(1) Work with the PO, Program Manager, Project Manager, ISO, and System Developer to address the rulemaking, IT program, and/or pilot project privacy issues that are identified through completion of the PTA;

(2) Work with the PO to finalize the PTA and prepare a PIA, if necessary;

(3) Obtain the Program and Project Manager's approval of PTA and PIA submissions;

(4) Submit PTAs and PIAs to the Privacy Service for review and approval; and

(5) Serve as point of contact for the system.

j. **System Developers.** System Developers will:

(1) Ensure that the system design and specifications conform to privacy standards and requirements; and

(2) Ensure that technical controls are in place for safeguarding PII and/or PHI from compromise or unauthorized access.

k. **Data Owners.** Data Owners will:

(1) Work with the POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions;

(2) Serve as point of contact for questions related to system data; and

(3) Respond to questions from POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers that are related PA submission.

l. **Information Security Officers (ISO).** ISOs will coordinate with their POs and System Managers to ensure that security risks are identified and documented in all PIA submissions. In addition, ISOs shall coordinate with their POs, their System Managers, and Privacy Service to ensure that the PIA(s) for each system is finalized.

m. **Privacy Officers (PO).** POs will coordinate with their local ISOs and System Managers to ensure that all data and associated risks are identified and documented in all PTA and PIA submissions. In addition, POs will work with their ISOs, System Managers, and Privacy Service to ensure that the PIA(s) for each system(s) immediate area of operation is of a quality that will reasonably ensure its approval by the Privacy Service PIA Support Team. PO's who are also identified and tasked by the Business Sponsor to be the IPT PO for PMAS programs or projects will review and make determinations whether or not a PIA is required for the program or project.

7. REFERENCES

a. Clinger-Cohen Act of 1996, 40 U.S.C. 1401 (Pub. L. 104-106, 110 Stat. 679 (1996)),

b. E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899 (2002)).

c. Federal Information Security Management Act (FISMA) of 2002 (Pub. L. 107-347, 116 Stat. 2946.

d. Paperwork Reduction Act of 1995 (as amended by Clinger-Cohen Act of 1996) (Pub. L. 104-13).

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

f. NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.

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

h. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems.

i. OMB Memo-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003).

j. VA Directive 6500, Managing Information Security Risk: VA Information Security Program.

k. VA Directive 6502, Enterprise-wide Privacy Program.

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

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

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

o. VA Handbook 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program.

8. 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. **Information Technology (IT).** Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(1) Of that equipment; or

(2) Of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.

c. **Integrated Project Team (IPT).** An IPT is a team of people with complementary skills and expertise who collaborate and commit to the timely delivery of specified work products.

d. **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.

e. **Personally Identifiable Information (PII).** A subcategory of VA Sensitive Data, PII means any information about the individual maintained by an agency, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history; and/or

(2) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records or any other personal information which is linked or linkable to an individual.

f. **Protected Health Information (PHI).** PHI is considered a subcategory of PII and SPI. PHI applies only to individually-identifiable health information that is under the control of Veterans Health Administration (VHA) or its business associates, as VA's only Covered Entity under Health Insurance Portability and Accountability Act (HIPAA). PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium. PHI excludes employment records held by an employer in its role as employer, records of a person deceased for more than 50 years, and some education records. It includes genetic information.

g. **Privacy Impact Assessment (PIA).** A PIA is an analysis that seeks to identify and mitigate the privacy and security risks associated with the use of SPI by a program, system, or practice. A PIA provides a framework for examining whether privacy, security and other vital data stewardship issues have been identified, addressed, and incorporated into the plan, design, operation, maintenance, and disposal of electronic information systems. PIAs are required to be performed in the conceptualization phase of the system lifecycle and updated whenever a system change could create a new privacy risk.

h. **Privacy Threshold Analysis (PTA)**. A PTA is used to identify IT systems, rulemakings, programs, or pilot projects that involve SPI and other activities that otherwise impact the privacy of individuals as determined by the Director, Privacy Service, and to assess whether there is a need for a PIA, whether a System of Records Notice is required, and if any other privacy requirements apply to the IT system. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what SPI is collected (and from whom) and how that information is used.

i. **Program.** A planned, coordinated group of projects, services, activities, procedures, etc., often for a specific purpose or designed to meet a public need.

j. **Program Manager.** An individual who devises and executes a plan of action aimed at accomplishing a clear objective, with details on what work is to be done, by whom, when, and what means or resources will be used.

k. **Project.** A set of interrelated tasks to be executed over a fixed period which creates a unique product or service.

l. **Project Manager.** An individual who arranges a set of interrelated tasks to be executed over a fixed period and within certain cost and other limitations.

m. **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. This term includes the amendment or repeal of an existing rule. An example of a rulemaking is the issuance or amendment of a regulation.

n. **System.** A working combination of hardware, software, and data communications devices.

o. **System Manager/System Owner.** A System Manager/System Owner is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The System Manager/System Owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements, the decision of who has access to the information system (and with what types of privileges or access rights) and the assurance that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

p. **Sensitive Personal Information (SPI).** Defined by 38 U.S.C. 5727(19) as any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) Information that can be used to distinguish or trace the individual’s identity, including name, social security number, date and place of birth, mother’s maiden name, or biometric records. For purposes of this handbook, the term SPI includes PII and PHI.