Department of Veterans Affairs
Washington DC, 20420

VA HANDBOOK 6300.5
Transmittal Sheet
August 3, 2017

PROCEDURES FOR ESTABLISHING AND MAINTAINING PRIVACY ACT SYSTEMS OF RECORDS

1. REASON FOR ISSUE: This handbook revises Department-wide procedures that implement policies contained in VA Directive 6300, Records and Information Management, for establishing and maintaining systems of records under the Privacy Act of 1974 and Office of Management and Budget (OMB) guidance, including OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This handbook updates procedures related to the establishment and maintenance of Privacy Act systems of records.

3. RESPONSIBLE OFFICE: The Assistant Secretary for Information and Technology (005), Deputy Chief Information Officer, Privacy and Risk (005PR); Associate Deputy Assistant Secretary Policy Planning & Incident Management (005R), Executive Director for Privacy (005P), Director, Office of Privacy, Information and Identity Protection (005P1), and VA Privacy Service (005P1A).

4. RELATED DIRECTIVE AND HANDBOOKS: VA Directive 6300, Records and Information Management; VA Directive 6502, VA Enterprise Privacy Program; VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act; VA Handbook 6300.7, Procedures for Computer Matching Programs; and VA Handbook 6300.1, Records Management Procedures.

5. RESCISSIONS: VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records, dated June 10, 2010; and VA Handbook 6502.4, Privacy Act Reviews, dated November 16, 2009.

CERTIFIED BY:

/s/
Dat P. Tran
Acting Assistant Secretary for
Office of Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
ROB C. THOMAS, II
Acting Assistant Secretary for OI&T
Chief Information Officer

Distribution: Electronic Only

PROCEDURES FOR ESTABLISHING AND MAINTAINING PRIVACY ACT SYSTEMS OF RECORDS

CONTENTS

PARAGRAPH **PAGE**

PROCEDURES FOR ESTABLISHING AND MAINTAINING PRIVACY ACT SYSTEMS OF RECORDS

1. PURPOSE

a. This handbook revises procedures for establishing and maintaining systems of records under the Privacy Act of 1974 (the Privacy Act). The Privacy Act requires agencies to "publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records" subject to the Act (5 U.S.C. 552a(e)(4)). The Privacy Act also requires agencies to send reports to Congress and the Office of Management and Budget (OMB) on the agency's intention to establish any new system of records and, under certain specified circumstances, the agency's intention to alter an existing system of records. This handbook provides guidance on the report and notice content, format, and distribution. It also describes the responsibilities of System Managers and situations when a report and notice are required.

b. In addition, OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* describes agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act and related OMB policies. The Circular supplements and clarifies existing OMB guidance.

2. RESPONSIBILITIES:

a. **The Secretary of Veterans Affairs.** The Privacy Act places principal responsibility for compliance with its provisions on Federal agencies. The head of each agency shall designate a Senior Agency Official for Privacy (SAOP). The head of each agency shall also ensure that the SAOP has the necessary resources to carry out his or her responsibilities.

b. **The Assistant Secretary for Information and Technology (ASIT).** The ASIT, as the SAOP has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals. At the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform particular functions that are assigned to the SAOP.

c. **VA Privacy Service.** Responsibilities of the VA Privacy Service include:

(1) Reviewing SORNs, narrative statements, supplementary documents, and congressional and OMB letters, ensuring that the documents meet the requirements of the Privacy Act and OMB guidance;

(2) Documenting and communicating the process for developing, approving, publishing, and maintaining a master inventory of SORNs;

(4) Assigning identifiers and numbers to new systems of records;

(5) Facilitating access to the RISC/OIRA Consolidated Information System (ROCIS) and assisting System Managers with entries into the system;

(6) Assisting System Managers with the process for drafting a SORN for all new, significantly altered, and rescinded systems of records;

(7) Assisting System Managers with drafting the appropriate narrative statement, supplementary documents, and congressional and OMB letters;

(8) Submitting the final signed SORN to the *Federal Register* for publication;

(9) Notifying the System Manager of comments received from the public;

(10) Publishing the list of VA's SORNs and all other required items on the VA Internet site; and

(11) Coordinating required Privacy Act Reviews and reporting findings as necessary to the SAOP.

d. **System Manager**. The Privacy Act requires that each agency designate an agency official who is responsible for each system of records. This person is known as the System Manager. The System Manager is usually the Information Owner, as defined by VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program. The System Manager is an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The System Manager is responsible for:

(1) Ensuring that the policies, practices, and procedures governing the maintenance of records in a system are being followed;

(2) Working with the Information Security Officer (ISO) to ensure appropriate management, operational, physical, administrative, and technical safeguards are in place to prevent unauthorized disclosure or alteration of information in the system, including a review of whether records are downloaded to a personal computer or removable storage devices (such as thumb drives, external hard drives, compact discs (CDs), digital versatile discs (DVDs), and cell phones) to be managed, stored or manipulated. Downloads such as these may lead to the creation of new, unauthorized systems of records;

(3) Confirming records contain only such information about an individual that is relevant and necessary to accomplish a purpose of the agency to be accomplished by statute or by Executive Order of the President;

(4) Ensuring the information in the system is accurate, timely, complete, relevant and necessary to accomplish a VA mission;

(5) Maintaining an accounting of disclosures;

(6) Guaranteeing routine uses are compatible with the purpose(s) for which the information was collected;

(7) Working with the Privacy Officer or designee to ensure that procedures for access, correction, or amendment of records conform to the requirements of this handbook, VA Handbook 6300.4, and VHA Handbook 1605.1, and that VA regulations governing the Privacy Act are followed;

(8) Conducting Privacy Act Reviews as described in section 7 of this handbook.

(9) Reviewing each system of records notice (SORN) biennially to ensure it accurately describes the system of records, and certifying to VA Privacy Service that the review was completed;

(10) Preparing new or altered system reports and related documents and ensuring that systems of records are not operated without first publishing the required notices and reports; republishing each SORN in its entirety every six years, regardless of whether there have been any changes to the system of records;

(11) Ensuring that the description of recordkeeping practices in the retention and disposal portion of the SORN reflects the retention and disposal of records approved by the Archivist of the United States. In the event there is no approved retention and disposal period for the records, immediate action must be initiated to obtain the approval of the Archivist of the United States. No record within the system of records may be destroyed until a records schedule is issued by the Archivist;

(12) Determining whether the system of records may be exempted from certain provisions of the Privacy Act (5 U.S.C. 552a(j) and (k)) and taking the necessary steps to invoke the exemptions. If the system of records is exempt, the exemption must be reviewed every three years to determine if the exemption is still needed; and

(13) Conducting detailed risk assessments of new or altered systems of records to ensure that appropriate administrative, technical, and physical safeguards are established to protect records in the system from unauthorized disclosure, alteration or access.

3. PUBLISHING SYSTEM OF RECORDS NOTICES

a. **General**. The Privacy Act requires agencies to publish a SORN in the *Federal Register* describing the existence and character of a new or modified system of records. A SORN is comprised of the *Federal Register* notice(s) that identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system. The requirement for agencies to publish a SORN allows the Federal Government to accomplish one of the basic objectives of the Privacy Act – fostering agency accountability through public notice.

b. **When to Publish a System of Records Notice**. Agencies are required to publish a SORN in the *Federal Register* when establishing a new system of records and must also

publish notice in the *Federal Register* when making significant changes to an existing system of records. As a general matter, significant changes are those that are substantive in nature and therefore warrant a revision of the SORN in order to provide notice to the public of the character of the modified system of records. The following are examples of significant changes:

(1) A substantial increase in the number, type, or category of individuals about whom records are maintained in the system. For example, a system covering physicians that is being expanded to include other types of health care providers (e.g., nurses or technicians) would require a revised SORN. Increases attributable to normal growth in a single category of individuals generally would not require a revised SORN.

(2) A change that expands the types or categories of records maintained in the system. For example, a benefit system that originally included only earned income information that is being expanded to include unearned income information would require a revised SORN.

(3) A change that modifies the scope of the system. For example, the combining of two or more existing systems of records.

(4) A change that modifies the purpose(s) for which the information in the system of records is maintained.

(5) A change in the agency's authority to maintain the system of records or maintain, collect, use, or disseminate the records in the system.

(6) A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute (*e.g.*, to seek access to or amendment of a record).

(7) A change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system. For example, a change in the access controls that substantially increases the accessibility of the information within the agency.

(8) A new routine use or significant change to an existing routine use that has the effect of expanding the availability of the information in the system.

(9) The promulgation of a rule to exempt a system of records from certain provisions of the Privacy Act (a Privacy Act exemption rule that is part of a report of a new or significantly modified system of records may also be reviewed by OMB under applicable regulatory review procedures - see section 6 of this handbook for information about Privacy Act exemption rules).

NOTE: This is not an exhaustive list of significant changes that would require a revised SORN. Other changes to a system of records would require a revised SORN if the changes are substantive in nature and therefore warrant additional notice. If there are questions about

whether particular changes to a system of records are significant, contact VA Privacy Service for assistance.

c. **What to Publish in a System of Records Notice**. Each notice of a new or modified system of records shall be drafted using the Office of the Federal Register SORN template, which is provided in Appendix II to OMB Circular A-108 or by contacting VA Privacy Service. While OMB allows agencies to publish partial revised SORNs, it is VA policy that all new and revised SORNs must be published in their entirety since the entire, revised SORN must be available to the public.

d. **Who Publishes a System of Records Notice**. The agency responsible for maintaining a system of records (including by providing for the operation of a system of records by a contractor on behalf of the agency) publishes the SORN. The exception to this requirement is in the case of a SORN for a government-wide system of records. For a government-wide system of records, the agency with government-wide responsibility shall publish the SORN (see section 6(i) of OMB Circular A-108 for information about government-wide systems of records).

NOTE: Publication shall occur at the Department or agency level, rather than the sub-agency, component, or program level. If a system of records will be maintained by an Administration or Program Office, VA Privacy Service shall publish the SORN.

e. **Timing of a System of Records Notice**. A new or revised SORN is effective upon publication in the Federal Register, with the exception of any new or significantly modified routine uses. VA may not publish a SORN in the *Federal Register* until it has provided advance notice of the proposal to OMB and Congress pursuant to the reporting instructions in section 4 of this handbook. New routines uses include any routine uses that VA is newly applying to the specific system, including routine uses that may already have been established for other systems of records.

(1) As soon as a SORN is published in the *Federal Register* VA may begin to operate the system of records – VA may collect, maintain, and use records in the system, and VA may disclose records pursuant to any of the conditions of disclosure in subsection (b) of the Privacy Act other than a new or significantly modified routine use. Any new or significantly modified routine uses require a minimum of 30 days after publication in the *Federal Register* before the routine uses are effective and may be used as the basis for disclosure of a record in the system.

(2) VA shall publish notice of any new or significantly modified routine use sufficiently in advance of the proposed effective date of the routine use to permit time for the public to comment and for VA to review those comments. In no circumstance may VA use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following *Federal Register* publication.

(3) If public comments are received on a published SORN, VA shall review the comments to determine whether any changes to the SORN are necessary. If VA determines the comments do not require a change, the SORN will become effective on the date as published in the SORN. If VA determines that significant changes to the SORN are necessary, VA shall publish

a revised SORN. If VA determines that significant changes to the routine uses or additional routine uses are necessary, VA shall provide an additional 30-day public comment and review period.

f. **Rescindment of a System of Records Notice**. When VA stops maintaining a previously established system of records, VA shall publish a notice of rescindment in the *Federal Register*. Each notice of rescindment shall be drafted using the *Office of the Federal Register Notice of Rescindment Template* (contact VA Privacy Service for the template). The notice of rescindment shall identify the system of records, explain why the SORN is being rescinded, and provide an account of what will happen to the records that were previously maintained in the system. If the records in the system of records will be combined with another system of records or maintained as part of a new system of records, the notice of rescindment shall direct members of the public to the SORN for the system that will include the relevant records. There are many reasons why VA may need to rescind a SORN. For example, the Privacy Act provides that an agency may only collect or maintain in its records information about individuals that is relevant and necessary to accomplish a purpose that is required by statute or executive order. If a system of records is comprised of records that no longer meet that standard, the Privacy Act may require that the agency stop maintaining the system and expunge the records in accordance with the requirements in the SORN and the applicable records retention or disposition schedule approved by the National Archives and Records Administration.

g. **Format and Style of a System of Records Notice**. System Managers shall draft SORNs in plain language with an appropriate level of detail to ensure that the public is properly informed about the character of the system of records. System Managers shall follow the publication format in the Office of the Federal Register SORN templates, which are provided in the appendices to OMB Circular A-108. In addition, VA shall consult the Office of the Federal Register's *Document Drafting Handbook (*http://www.archives.gov/federal-register/write/handbook/) for general guidance on drafting *Federal Register* notices.

h. ***Scope of a System of Records***. The Privacy Act requires agencies to publish a separate SORN for each system of records. Before developing a SORN, VA shall carefully consider the proper scope of the system of records. VA has discretion in determining what constitutes a system of records for purposes of preparing a notice. However, VA shall consider the following general factors when determining whether a group of records will be treated as a single system or multiple systems for the purposes of the Privacy Act:

(1) The agency's ability to comply with the requirements of the Privacy Act and facilitate the exercise of the rights of individuals.

(2) The informative value of the notice. VA shall consider whether a single SORN or multiple SORNs would provide the most informative notice to the public about the existence and character of the system(s).

(3) The agency's ability to be responsive to individual access requests. VA shall consider whether a single SORN or multiple SORNs would provide the best notice to individuals regarding how and where they may request access to their records maintained in the system(s) and would allow the agency to most effectively respond to such requests.

(4) The purpose(s) and use(s) of the records. If different groups of records are used for distinct purposes, it may be appropriate to treat those different groups of records as separate systems. Although different groups of records may serve a general common purpose, VA shall also consider whether different routine uses or security requirements apply to the different groups, or whether the groups are regularly accessed by different employees of the agency.

(5) The cost and convenience to the agency, but only to the extent consistent with the above considerations regarding compliance and individual rights.

NOTE: Considerable latitude is left to agencies in defining the scope or grouping of records that constitute a system of records. An agency may choose to consider the entire group of records for a particular program as a single system, or the agency may consider it appropriate to segment a group of records (*e.g.,* by function or geographic unit) and treat each segment as a system of records to provide better notice to the public. When an agency chooses to segment a group of records into separate systems of records, the agency shall nevertheless ensure that the SORN for each segment clearly describes any linkages that exist between the different systems of records based on the retrieval of the records. For example, if records described in different SORNs are in fact linked together through a central indexing or retrieval capability such that an employee or contractor retrieving records described in one SORN would necessarily also retrieve and gain access to records described in another SORN, VA shall explain this linkage in the “Policies and Practices for Retrieval of Records” section of both SORNs.

i. **Government-Wide System of Records**. A government-wide system of records is a system of records where one agency has regulatory authority over records in the custody of multiple agencies, and the agency with regulatory authority publishes a SORN that applies to all of the records regardless of their custodial location.

(1) The application of a government-wide SORN ensures that privacy practices with respect to the records are carried out uniformly across the Federal Government in accordance with the rules of the responsible agency. For a government-wide system of records, all agencies – not just the agency with government-wide responsibilities – are responsible for complying with the terms of the SORN and the applicable requirements in the Privacy Act, including the access and amendment provisions that apply to records under an agency’s control.

(2) As a general matter, a government-wide system of records is appropriate when one agency has government-wide responsibilities that involve administrative or personnel records maintained by other agencies. For example, the Office of Personnel Management has published a number of government-wide SORNs relating to the operation of the Federal Government’s personnel programs. Agencies shall coordinate with OMB’s Office of Information and Regulatory Affairs (OIRA) whenever they are considering the need for a new government-wide system of records.

(3) All government-wide systems of records necessarily affect multiple agencies that will have custody of the records in the system. Accordingly, one step of OMB’s review of a new or modified government-wide system of records will involve an interagency review process that allows other affected agencies to review the proposal and provide comments. Once the agency with regulatory authority has published a government-wide SORN, no other agency

shall publish a SORN that duplicates the existing government-wide SORN, unless such publication has been approved by OMB.

j. **System of Records Operated by a Contractor**.

(1) When VA provides by contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, VA shall cause the requirements of the Privacy Act to be applied to the system, limited only by VA's authority to do so. In such cases, the system operated by the contractor is, in effect, deemed to be maintained by VA. VA shall publish a SORN for the system, establish an appropriate routine use to permit disclosure of records to the contractor for the purpose of operating the system, and, to the extent consistent with VA's authority, incorporate enforceable clauses in the contract and statement of work to ensure that the contractor complies with all applicable requirements of the statute and OMB policies.

NOTE: In cases where VA acts as a service provider for one or multiple agencies, all agencies involved must ensure compliance with applicable Privacy Act requirements.

(2) Agencies shall design their procurement practices to ensure that all contracts that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals are reviewed and approved by the SAOP before award to help evaluate whether a system of records will be established and, if so, to include appropriate clauses in the contract. The SAOP shall have access to a complete and accurate list of all of the agency's contracts involving information that identifies and is about individuals, and shall establish a process to ensure that the language of each contract is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees consistent with the agency's authority.

k. **Routine Uses.** A routine use is a particular kind of disclosure of a record outside of the agency maintaining the system of records. To qualify as a routine use, the disclosure must be for a purpose that is compatible with the purpose for which the information was originally collected. The routine use provision of the Privacy Act functions as one of the exceptions to the statute's general prohibition against the disclosure of a record without the written consent of the individual to whom the record pertains.

(1) The Privacy Act requires agencies to describe each routine use of the records contained in the system of records, including the categories of users of the records and the purpose of the use. VA may only establish routine uses for a system by explicitly publishing the routine uses in the relevant SORN. When drafting a SORN, System Managers should contact VA Privacy Service for an inventory of routine uses as drafted by VA Office of the General

Counsel. VA is strongly encouraged to publish all routine uses applicable to a system of records in a single *Federal Register* notice for that system. However, some agencies choose to publish a separate notice of routine uses that are applicable to many systems of records at the agency, and then incorporate them by reference into the notices for specific systems to which they apply. When incorporating such routine uses by reference, VA shall ensure that the routine use section of the SORN clearly indicates which of the separately published routine

uses apply to the system of records and includes the *Federal Register* citation where they have been published.

(2) Routine uses shall be narrowly tailored to address a specific and appropriate use of the records. VA shall describe each routine use with sufficient clarity and specificity to ensure that members of the public who are unfamiliar with the system or the agency's program can understand the uses to which the records are subject. Overly broad or ambiguous language would undermine the purpose of the routine use notice requirement and shall be avoided. A routine use that only applies to certain records in a system of records should indicate its limited scope.

(3) Before establishing a routine use, VA must determine that it has the necessary authority to make disclosures under the routine use and that the routine use is appropriate. As explained in OMB's Privacy Act Guidelines, a routine use may be appropriate when the use of the record is necessary for the efficient conduct of government, and when the use is both *related to* and *compatible with* the original purpose for which the information was collected (*e.g.,* the development of a sampling frame for an evaluation study or other statistical purposes). Moreover, the concept of compatibility comprises both *functionally equivalent* uses of the information as well as other uses of the information that are *necessary and proper* (e.g., a disclosure to the National Archives and Records Administration to conduct records management activities pursuant to specific statutory authority).

(4) VA shall publish notice of any new or significantly modified routine uses sufficiently in advance of the proposed effective date of the routine uses to permit time for the public to comment and for VA to review those comments. In all cases, the Privacy Act requires agencies to publish any new or modified routine use at least 30 days before the effective date of the routine use. VA shall not disclose any records pursuant to a new or modified routine use until after the 30-day comment period has ended and VA has considered any comments from the public and determined that no further modifications are necessary.

(5) If VA determines that an existing routine use is no longer necessary or appropriate, VA shall immediately discontinue all disclosures under the routine use and shall publish a revised SORN in the *Federal Register* rescinding the routine use. Moreover, if VA determines that the routine uses in a SORN do not accurately and completely describe all routine use disclosures to which the records in the system are subject, VA shall discontinue any disclosures that are not accurately and completely described and revise the routine uses in the SORN to accurately and completely describe those disclosures.

l. **Information Collections and Privacy Act Statements**. If VA will be collecting information as part of a new or modified system of records, VA may need to comply with additional

requirements, including those in the Paperwork Reduction Act, the E-Government Act of 2002, and related OMB guidance. VA (and their contractors) shall meet all applicable requirements before they begin collecting the information. For guidance on whether and how these statutes and OMB policies apply to a collection activity, VA shall consult OMB guidance and contact OIRA. If VA asks individuals to supply information that will become part of a system of records, VA is required to provide a Privacy Act statement on the form used to collect the information or on a separate form that can be retained by the individual.

(1) VA shall provide a Privacy Act statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond.

NOTE: When information is collected over the telephone, VA shall orally provide the required information and provide a means by which the individual can receive the information in writing.

(2) The Privacy Act statement shall include a plain-language description of:

(a) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(b) the principal purpose(s) for which the information is intended to be used;

(c) the published routine uses to which the information is subject;

(d) the effects on the individual, if any, of not providing all or any part of the requested information; and

(e) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

NOTE: When describing the routine uses in the Privacy Act statement, VA shall tailor the scope and content of the description in order to provide the most effective notice to the public. VA generally need not restate the full text of the published routine uses or provide a lengthy list of routine uses to which the information is subject. Rather, VA may provide a plain-language summary of the routine uses and provide a link to the website where the full list of routine uses is available.

4. REPORTING SYSTEMS OF RECORDS TO OMB AND CONGRESS

a. **General**. The Privacy Act requires each agency that proposes to establish or significantly modify a system of records to provide adequate advance notice of any such proposal to OMB, the Committee on Oversight and Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate. This advance notice is separate from the public comment period for new or modified routine uses required by

subsection (e)(11) of the Privacy Act and discussed in section 3 of this handbook. Agencies provide advance notice to OMB and the committees of jurisdiction in Congress in order to permit an evaluation of the probable or potential effect of such a proposal on the privacy or other rights of individuals.

b. **Advance Notice of a New or Modified System of Records**. VA shall report to OMB and Congress any proposal to establish or significantly modify a system of records at least 30 days prior to the submission of the notice to the *Federal Register* for publication. OMB will have 30 days to review the proposal and provide any comments to the agency. The 30-day review

period is separate from – and may not run concurrently with – the publication period in the *Federal Register*. Only significant changes to a system of records that require a revision to the SORN, as described in section 3 of this handbook, need to be reported to OMB and Congress; changes that are not significant do not need to be reported.

(1) Advance notice to OMB and Congress is required by subsection (r) of the Privacy Act. The purpose of the advance notice to OMB and Congress is to permit an evaluation of the potential effect of the proposal on the privacy and other rights of individuals. Although the review period will generally require no more than 30 days, OMB has the discretion to extend the 30-day review period based on the specific circumstances of the proposal. If VA has questions about the timing of the review, VA shall consult with OIRA.

(2) In circumstances where it is not feasible for the agency to wait until the 30-day review period for OMB and Congress has expired to publish the notice in the *Federal Register*, VA may submit a formal written request from the SAOP to OIRA for an expedited advance review period (see section 4(d) of this handbook for information about expedited review requests).

Illustration of Standard Review Process for Systems of Records
(The actual timing of the process will depend on the specific circumstances of the proposal, the internal review and clearance procedures, the review process for any Privacy Act exemption rules, and the logistics of *Federal Register* publication.)

Agency Action	Explanation	Timing
VA submits report to OMB and Congress at least 30 days before publication of the notice in the *Federal Register*.	OMB and Congress have the opportunity to evaluate the probable or potential effect of such a proposal on the privacy or other rights of individuals.	Day 1
After incorporating any comments from OMB – and unless OMB provides instructions to the contrary – VA may publish the notice in the *Federal Register* and solicit comments from the public.	Notices published in the *Federal Register* after review by OMB and Congress are effective upon publication, with the exception of any new or modified routine uses. New or modified routine uses require a minimum of 30 days after publication in the *Federal Register* before they can become effective.	Day 31
The 30-day public comment period closes and VA reviews and considers any comments received. If no changes to the notice are necessary, the notice remains effective and any new or modified routine uses become effective.	If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary. If VA determines that significant changes are necessary, VA will need to begin the review process again.	Day 61

c. **Instructions for Reporting a New or Modified System of Records**. Agencies are required to report to OMB and Congress any proposal to establish or significantly modify a system of records. Agencies shall report proposals to the committees of jurisdiction in Congress by messenger or by mailing the reports to the addresses provided below. VA shall report proposals to OMB using OMB's specific web-based portal, as described below. VA shall not mail or messenger paper versions of the report to OMB. Submission of the report to OMB will officially start the 30-day advance review period.

(1) *House of Representatives*. VA shall submit reports to the chair of the House Committee on Oversight and Government Reform, 2157 Rayburn House Office Building, Washington, DC 20515.

(2) *Senate*. VA shall submit reports to the chair of the Senate Committee on Homeland Security and Governmental Affairs, 340 Dirksen Senate Office Building, Washington, DC 20510.

(3) *OMB*. VA shall submit reports to OMB using the web-based portal jointly developed by OIRA and the General Services Administration's (GSA) Regulatory Information Service Center

(RISC). This web-based portal, the RISC/OIRA Consolidated Information System (ROCIS), was developed to facilitate the submission and review of regulations and other agency materials (https://www.rocis.gov). For detailed instructions on how to use ROCIS to submit reports to OMB, VA shall consult the user manuals available on the ROCIS website or register for the training classes conducted by RISC at GSA headquarters.

d. ***Request for Expedited Review of a New or Modified System of Records***. Although VA is required to provide adequate advance notice of any proposal to establish or significantly modify a system of records, there may be circumstances where it is not feasible for the agency to wait until the 30-day review period has expired to publish a notice in the *Federal Register*. In such cases, VA may submit a formal written request from the SAOP to OIRA for an expedited OMB review period.

(1) The request shall be included in the transmittal letter that VA submits to OIRA in ROCIS. The request shall demonstrate VA's specific and compelling need for the expedited review, indicate why VA cannot meet the established review period, and explain the consequences if the request is not granted.

(2) When OIRA grants VA's request for expedited review, VA will be allowed to publish the notice in the *Federal Register* after the expedited OMB review period. When OIRA does not grant VA's request for expedited review, the normal OMB review process will proceed. OMB may not waive the explicit requirement in the Privacy Act for a 30-day *Federal Register* public notice before the adoption of a new or modified routine use, nor may OMB waive the adequate advance notice that is required to Congress.

e. **Content of the Report of a New or Modified System of Records**. The report of a new or significantly modified system of records includes a transmittal letter, a narrative statement, a draft *Federal Register* notice, any Privacy Act exemption rules, and any supplementary documents.

(1) *Transmittal Letter*. The transmittal letter serves as a brief cover letter accompanying the report. The transmittal letter shall:

(a) Be signed by the SAOP.

(b) Contain the name, email address, and telephone number of the individual who can best answer questions about the proposed system of records.

(c) Contain VA's assurance that the proposed system of records fully complies with the Privacy Act and OMB policies.

(d) Contain VA's assurance that the proposed system of records does not duplicate any existing agency or government-wide systems of records.

(2) *Narrative Statement*. The narrative statement provides a brief overview of the proposed system of records making reference to the other materials in the report without simply restating information provided in those materials. The narrative statement shall:

(a) Describe the purpose(s) for which VA is establishing or modifying the system of records and explain how the scope of the system is commensurate with the purpose(s) of the system.

(b) Identify the specific authority (statute or executive order) under which the system of records will be maintained. VA shall avoid citing authority that is overly general; rather, VA shall cite the specific programmatic authority for collecting, maintaining, using, and disseminating the information.

(c) An evaluation of the probable or potential effect of the proposal on the privacy of individuals whose information will be maintained in the system of records. If VA has conducted one or more privacy impact assessment(s) with respect to information technology that will be used to collect, maintain, or disseminate the information in the system of records, the privacy impact assessment(s) will likely provide the information necessary to meet this requirement, and may be submitted in lieu of drafting a separate evaluation.

(d) Explain how each new or modified routine use satisfies the compatibility requirement of the Privacy Act.

(e) Identify any information collections approved by OMB or submitted to OMB for approval that will be used to collect information that will be maintained in the system of records, and provide the relevant names, OMB control numbers, and expiration dates. If the request for OMB approval of an information collection is pending, VA may simply state the name of the collection and the date it was submitted to OMB for review.

(3) *Federal Register Notice*. The draft new or revised notice in the format prescribed by the Office of the Federal Register SORN template, which is provided in the Appendix II to OMB Circular A-108.

(4) *Exemption Rule*. Any new Privacy Act exemption rules or changes to published exemption rules in *Federal Register* format that VA proposes to issue that will apply to records in the new or significantly modified system of records.

(5) *Supplementary Documents*. The supplementary documents include:

(a) For significantly modified systems, VA shall include a list of the substantive changes to the previously published version of the notice and/or a version of the previously published notice that has been marked up to show the changes that are being proposed.

(b) VA shall include any other supplementary documents requested by OMB.

f. **Reporting General Changes to Multiple Systems of Records**. When VA makes a general change to its programs or information technology that applies in a similar way to

multiple systems of records (*e.g.*, enabling remote access to systems, moving systems from a conventional data center to a cloud-based storage environment, adding a routine use to all systems of records), VA may submit a single, consolidated report to OMB and Congress describing the changes. However, VA shall ensure that any changes are properly reflected in all published SORNs.

5. PRIVACY ACT IMPLEMENTATION RULES

a. **Rulemaking.** Each agency that maintains a system of records shall promulgate rules, in accordance with the rulemaking procedures in 5 U.S.C. § 553, to implement the requirements of the Privacy Act. Privacy Act implementation rules shall provide the public with sufficient information to understand how an agency is complying with the law, and provide sufficient information for individuals to exercise their rights under the law. In particular, VA's Privacy Act implementation rules shall:

(1) establish procedures whereby an individual can be notified in response to his or her request if any system of records named by the individual contains a record pertaining to him or her;

(2) define reasonable times, places, and requirements for authenticating the identity of an individual who requests his or her record or information pertaining to him or her before the agency makes the record or information available to the individual (more rigorous authentication procedures may be required for more sensitive records);

(3) establish procedures whereby an individual can be notified at his or her request how the individual can gain access to any record pertaining to him or her in the system, including special procedures, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him or her;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to him or her, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his or her rights under the Privacy Act; and

(5) establish fees to be charged, if any, to any individual for making copies of his or her record, excluding the cost of any search for and review of the record.

b. **OMB Review**. VA shall submit proposed and final Privacy Act implementation rules to OMB if those rules are subject to OMB review under Executive Order 12866, *Regulatory Planning and Review*, Executive Order 13563, *Improving Regulation and Regulatory Review*, or other regulatory review procedures.

6. PRIVACY ACT EXEMPTION RULES

a. **Exemption Rules**. The Privacy Act includes two sets of provisions that allow agencies to claim exemptions from certain requirements in the statute. These provisions allow agencies in certain circumstances to promulgate rules, in accordance with 5 U.S.C. § 553, to exempt a system of records from select provisions of the Privacy Act. If VA wishes to promulgate a rule to exempt a system of records, it shall follow all applicable rulemaking procedures. Generally, these procedures will require agencies to publish in the *Federal Register* a proposed rule soliciting comments from the public, followed by a final rule. At a minimum, the Privacy Act exemption rules shall include:

(1) The specific name(s) of any system(s) that will be exempt pursuant to the rule (the name(s) shall be the same as the name(s) given in the relevant SORN(s));

(b) The specific provisions of the Privacy Act from which the system(s) of records is to be exempted and the reasons for the exemption (a separate reason need not be stated for each provision from which a system is being exempted, where a single explanation will serve to explain the entire exemption); and

(c) An explanation for why the exemption is both necessary and appropriate.

b. **SORN Revision**. In addition to promulgating a rule, if VA wishes to claim an exemption for a system of records, it shall also identify the applicable exemption(s) in the relevant SORN. Whenever VA publishes a rule to claim a new or revised exemption for a system of records, it shall also revise the SORN pursuant to the publication requirements described in section 3 of this handbook, and report the proposal to OMB and Congress pursuant to the reporting requirements described in section 4 of this handbook.

c. **OMB Review**. When VA wishes to promulgate a Privacy Act exemption rule, it shall submit the draft rule to OMB along with the new or revised SORN(s) associated with the systems that VA wishes to exempt (see section 4 of this handbook for information about reporting a new or modified system of records). In most cases a separate submission of the rule to OMB will not be required and OMB will review the proposed exemption rule along with the SORN. However, in some exceptional cases exemption rules may also be subject to OMB's regulatory review procedures under Executive Order 12866, *Regulatory Planning and Review*, and Executive Order 13563, *Improving Regulation and Regulatory Review*. In such cases, OIRA will notify VA as soon as possible regarding the appropriate review process.

d. **Exemption Must be Necessary and Appropriate**. It is important to recognize that Privacy Act exemptions are permissive. Even in circumstances where VA is authorized to promulgate an exemption, it shall only do so if the exemption is necessary and consistent with established policies. Moreover, while the Privacy Act allows agencies to promulgate exemptions that apply at the system level, agencies shall exempt only those records in a system of records for which the exemption is necessary and appropriate. In cases where it is necessary to maintain exempt and non-exempt records in a single system of records, agencies shall only exempt the records for which the exemption is necessary and appropriate.

e. **Reporting and Publication.** VA may not exempt any system of records from any provision of the Privacy Act until all of the applicable reporting and publication requirements have been met.

7. PRIVACY ACT REVIEWS

a. **SORN Requirements in OMB Circular A-130**. Circular A-130 outlines privacy requirements that apply to the information system development life cycle. Because all information in systems of records is part of one or more information systems, many of the requirements in Circular A-130 apply to systems of records. For example, agencies are required to select, implement, and assess privacy controls and develop privacy plans for information systems. In addition, agencies are required to establish and maintain an agency-

wide privacy continuous monitoring (PCM) program, based on a written PCM strategy. The requirement to establish and maintain a PCM program has replaced the prior OMB requirement for agencies to conduct annual Privacy Act reviews.

b. **Privacy Controls**. During the development of an information system, VA shall select, implement, and assess privacy controls that allow VA to ensure continued compliance with all applicable requirements in the Privacy Act and related OMB guidance. Furthermore, VA shall monitor and assess privacy controls selected for an information system on an ongoing basis. This includes assessing the effectiveness of the privacy controls, documenting changes to the information system, analyzing the privacy impact associated with the changes, and reporting the state of the information system to appropriate agency officials. The type, rigor, and frequency of control assessments shall be sufficient to account for risks that change over time based on changes in the threat environment, agency missions and business functions, personnel, technology, or environments of operation. VA shall design its privacy control selection process to include privacy controls that allow it to ensure compliance with applicable requirements in the Privacy Act and related OMB guidance. At a minimum, the controls selected for an information system that contains information in a system of records shall address the following elements:

(1) Minimization. VA shall ensure that no system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order.

(2) *Systems of Records Notices*. VA shall ensure that all SORNs remain accurate, up-to-date, and appropriately scoped (see section 3(h) of this handbook for information about the scope of a system of records); that all SORNs are published in the *Federal Register*; that all SORNs include the information required by the Circular; and that all significant changes to SORNs have been reported to OMB and Congress (see section 4 of this handbook for information about reporting a modified system of records).

(3) Routine Uses. VA shall ensure that all routine uses remain appropriate and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected (see section 3(k) of this handbook for information about routine uses).

(4) Privacy Act Exemptions. VA shall ensure that each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary (see section 6 of this handbook for information about Privacy Act exemptions).

(5) Contracts. VA shall ensure that the language of each contract that involves the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals, is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees (see section 3(j) of this handbook for information about systems of records operated by contractors).

(6) Privacy Training. VA shall ensure that its training practices are sufficient and that agency personnel understand the requirements of the Privacy Act, OMB guidance, VA's implementing regulations and policies, and any job-specific requirements.

c. **VA Privacy Act Reviews**. In order to comply with the requirements of the Privacy Act and OMB guidance, VA will conduct a review of each SORN biennially (from the date of publication in the *Federal Register*). The System Manager will complete the review and return a signed checklist to VA Privacy Service. If there have been significant changes, the System Manager will prepare the documents to republish the SORN in its entirety. If the system is obsolete, the System Manager will prepare the notice of rescindment. Every six years (from the date of publication) the System Manager will republish the SORN in its entirety even if there have been no significant changes. VA Privacy Service will report any significant findings to the SAOP.

8. ANNUAL FISMA PRIVACY REVIEW AND REPORT

The Privacy Act originally required the President to submit a biennial report to Congress describing the administration of the statute. However, this requirement was subsequently repealed. In place of the biennial Privacy Act report, OMB now reports to Congress on agencies' compliance with privacy requirements through the annual Federal Information Security Modernization Act of 2014 (FISMA) report to Congress. Each year, OMB issues guidance instructing each SAOP to review the administration of the agency's privacy program and report compliance data to OMB. OMB uses the reports from agencies to develop its annual FISMA report to Congress.

9. AGENCY WIBSITE POSTING

VA shall maintain a central resource page dedicated to its privacy program on its principal website at www.va.gov/privacy. At a minimum, VA shall include the following materials related to the Privacy Act on its central privacy program page:

a. **System of records notices**. VA shall list and provide links to complete, up-to-date versions of all agency SORNs. This requires VA to provide the following:

(1) A list of all of the VA's systems of records;

(2) Citations and links to all *Federal Register* notices that comprise the SORN for each system of records; and

(3) For any SORNs that are comprised of multiple *Federal Register* notices, an unofficial consolidated version of the SORN that describes the current system of records and allows members of the public to view the SORN in its entirety in a single location.

NOTE: The requirement for VA to provide links to complete, up-to-date versions of SORNs on the VA's privacy program page does not replace the Privacy Act's statutory requirement for VA to publish SORNs in the *Federal Register*. Notice in the Federal Register of the establishment of a system of records will continue to serve as VA's official notice (see section 3 of this handbook for information about publishing SORNs).

b. **Exemptions to the Privacy Act**. VA shall provide citations and links to the final rules published in the *Federal Register* that promulgate each Privacy Act exemption claimed for its systems of records (see section 6 of this handbook for information about Privacy Act exemption rules).

c. **Privacy Act implementation rules**. VA shall list and provide links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f) (see section 5 of this handbook for information about Privacy Act implementation rules).

d. **Instructions for submitting a Privacy Act request**. VA shall provide instructions in clear and plain language for individuals who wish to request access to or amendment of their records pursuant to 5 U.S.C. § 552a(d).

This is not an exhaustive list of the materials that VA is required to include on its central privacy program page. VA shall refer to other OMB guidance documents to understand all website posting requirements.

10. VA PRIVACY SERVICE CONTACT INFO

a. Hotline: 202-273-5070

b. Mailbox: privacyservice@va.gov

11. DEFINITIONS

a. **Disclosure.** Providing information from a system of records, by any means, to anyone other than the individual by whose name or other identifier the record is retrieved.

b. **Individual.** A living citizen of the United States or an alien lawfully admitted for permanent residence. The definition of "individual" for Privacy Act purposes differs from the definition of "individual" for Freedom of Information Act (FOIA) purposes. Deceased persons, non-resident aliens, businesses, and organizations are not "individuals" under the Privacy Act.

c. **Maintain.** To collect, keep, use, disseminate, or any combination of these recordkeeping functions. As used in the Privacy Act, VA regulations, and this handbook, this word connotes control over and, therefore, responsibility and accountability for systems of records.

d. **Record.** Any item, collection, or grouping of information about an individual that is maintained by the Department, such as, but not limited to, individuals education, financial transactions, personal history, or medical history, and that contains individuals name or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voice print or a photograph. The definition does not distinguish between data and information. Both are within the scope of the definition.

e. **Routine use**. This term is unique to the Privacy Act and means the disclosure of a record for a reason that is compatible with the purpose for which it was collected. A routine use is one that is relatable and necessary to a purpose for collecting the record. To be effective, a routine use must be properly published in the *Federal Register*.

e. **Senior Agency Official for Privacy (SAOP)**. The senior official, designated by the head of the Department, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

f. **System Manager**. An official who is responsible for the management, operation, and release of information from a system of records subject to the Privacy Act. The System Manager is usually the Information Owner, as defined by VA Handbook 6500. The System Manager is an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

g. **System of records**. Any group of records under the control of an 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. A record in a system of records must contain two elements: a personal identifier and at least one item of personal information. If a retrieval of personal information is possible, but not actually done, or if it depends on memory or a sequential search, the collection of records is not a system of records. However, creating a retrieval method or cross-index arranged by personal identifier for randomly filed records makes that record collection a system subject to the provisions of the Act.

f. **System of records notice (SORN)**. The notice(s) published by an agency in the *Federal Register* upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in OMB Circular A-108. As explained in OMB Circular A-108, a SORN may be comprised of a single *Federal Register* notice addressing all of the required elements that describe the current system of records, or it may be comprised of multiple *Federal Register* notices that together address all of the required elements. A SORN is required when all of the following apply:

- Records are maintained by a Federal agency, and
- The records contain information about an individual, and
- The records are retrieved by name or personal identifier.

APPENDIX A - VA SORN APPROVAL PROCESS

Before drafting a SORN, System Managers may contact the VA Privacy Service (005P1A) at (202) 273-5070, or by email to privacyservice@va.gov to coordinate SORN efforts.

Step 1. If it is a new SORN, the System Manager contacts VA Privacy Service (005P1A) to receive a SOR number. If it is an amended SORN, the System Manager will use the existing SOR number. The SOR number consists of the next sequential number, plus the letters "VA" and the mail routing symbol of the originating office (e.g., 146VA005Q3). The routing symbol may change in subsequent publications of the SORN. There is no limit on how many characters the SOR number can have.

Step 2. The System Manager drafts the appropriate documents (see table below). Contact VA Privacy Service for templates. Note that only significantly modified SORNs or SORNs that modify routine uses are subject to OMB and congressional review and public comment.

Step 3. The System Manager then creates a SORN submission package in the VA document management system (VA Intranet Quorum 3- VAIQ), loads the documents to the "Documents" tab, and makes assignments to the appropriate offices for concurrence on the Concurrence and Summary Sheet (VA Form 4265).

.	New SORN	Significantly modified SORN or routine uses (see section 3e)	Not significantly modified nor routine uses	Rescinded SORN
Comment period required	Yes	Yes	No	No
SORN (use OMB template for full notice)	Yes	Yes	Yes	Yes
Transmittal Letters (see section 4e(1))	Yes	Yes	No	No
Narrative Statement, including information from the privacy impact assessment (see section 4e(2))	Yes	Yes	No	No
Exemption Rule (see section 4e(4))	Yes, if applicable	Yes, if applicable	No	No
Supplementary Documents, including marked-up version of previous SORN (see section 4e(5))	Yes, if applicable	Yes	No	No
Form 0907	Yes	Yes	Yes	Yes
Concurrences (in addition to System Manager's internal process)	OCLA (009) OGC (02)	OCLA (009) OGC (02)	OGC (02)	OGC (02)

Step 4. Once the concurrences are obtained, the System Manager prepares a hard copy folder, makes an assignment to VA Privacy Service (005P1A), with a 90-day due date, and routes the folder to (005P1A). VA Privacy Service reviews all SORN packages and recommends approval to the Assistant Secretary for Information and Technology (AS/IT) (005).

Step 5. The AS/IT approves the package and signs the letters.

Step 6. VA Privacy Service routes the package to the Office of Executive Correspondence (001B) to process for the Secretary's (or designee's) signature.

Step 7. Once the Secretary (or designee) signs the SORN, VA Privacy Service is notified.

Step 8. For new SORNs or significantly modified SORNs, VA Privacy Service notifies the System Manager to upload the signed SORN and related documents into RISC/OIRA Consolidated Information System (ROCIS). VA Privacy Service will upload the signed letter and submit the package electronically to OMB. VA Privacy Service also forwards packages to OCLA (009) for dispatch to addressed members Congress.

Step 9. For new SORNs or significantly modified SORNs, OMB and members of Congress have 30 days to review and comment (does not run concurrently with the public comment period). If there are no comments or if the SORN was not subject to OMB and congressional review, VA Privacy Service transmits the SORN to the *Federal Register* for publication. VA Privacy Service will receive notification of any public comments from the Office of Regulation Policy and Management (00REG), and will send them to the System Manager, who must review and determine if revisions to the SORN are warranted.

Step 10. Once the SORN is published it will be posted to the VA Internet site, www.va.gov/privacy by the VA Privacy Service.

A-2