PROCEDURES FOR ESTABLISHING AND MAINTAINING PRIVACY ACT SYSTEMS OF RECORDS

1. REASON FOR ISSUE: This handbook implements policies contained in the Department of Veterans Affairs (VA) Directive 6502, VA Enterprise Privacy Program, 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 replaces VA Handbook 6300.5 and is aligned under VA Directive 6502, VA Enterprise Privacy Program. It sets forth the following policy changes:

a. Clarify the responsibilities of the System Managers or designees for each system of records (SOR), as well as VA's Privacy Service.

b. Eliminate the roles of Assistant Secretary of Information and Technology, Chief Privacy Officer and Director, VA Privacy Service, as these roles are addressed in VA Directive 6502.

3. RESPONSIBLE OFFICE: The Assistant Secretary for Information and Technology (005), Deputy Chief Information Officer, Compliance, Risk and Remediation (005X); Deputy Chief Information Officer FOIA, Records and Assessment Compliance (005X), and VA Privacy Service (005X6F).

4. **RELATED DIRECTIVES AND HANDBOOKS:** VA Directive 6502, VA Enterprise Privacy Program; VA Handbook 6502.4, Procedures for Computer Matching Programs; VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act; VA Directive 6508, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment, VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program.

5. **RESCISSION:** VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records, dated August 3, 2017.

CERTIFIED BY:

/s/
Guy Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt D. DelBene
Assistant Secretary for
Information and Technology and
Chief Information Officer

DISTRIBUTION: Electronic Only

PROCEDURES FOR ESTABLISHING AND MAINTAINING PRIVACY ACT SYSTEMS OF RECORDS

TABLE OF CONTENTS

PROCEDURES FOR ESTABLISHING AND MAINTAINING PRIVACY ACT SYSTEMS OF RECORDS

1. **PURPOSE.**

   a. This handbook directs procedures for establishing, amending and maintaining systems of records under the Privacy Act of 1974 (5 U.S.C. § 552a, the 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 OMB on the agency's intention to establish any new SOR and, under certain specified circumstances, the agency’s intention to alter or rescind an existing SOR. This handbook provides guidance on the report and notice content, format and distribution. It also describes the responsibilities of System Managers or designee and situations when a System of Records Notice (SORN) is required.

   b. In addition, OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act and OMB Memorandum 99-05 describe 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.

   c. This Procedure for establishing and maintaining Privacy Act System of Records process ensures that information security is addressed throughout the life cycle of each agency information system (IAW FISMA 44 USC (b) (2) (C)).

2. **RESPONSIBILITIES.**

   a. **System Managers for VA Administrations and Staff Offices.** The Privacy Act requires that each agency designate an agency official responsible for each SOR. This person is known as the System Manager. The System Manager is usually the Information Owner/Steward, as defined by VA Handbook 6500, Risk Management Framework for VA Information Systems – VA Information Security Program. In cases where the System Manager is not the Information Owner/Steward, the Information Owner/Steward may designate a System Manager. In this instance, the System Manager will communicate all key decisions concerning the SOR with the Information Owner/Steward. The System Manager is an official with statutory or operational authority for specified information and for establishing the controls for its generation, collection, processing, dissemination and disposal. The System Manager may designate another VA staff member or contractor to fulfill the duties outlined in this handbook. The System Manager or designee shall:

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

(2) Confirm 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;

(3) Work with Records Officer to ensure 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 at NARA Records Schedule | National Archives.

(4) Maintain an accounting of disclosures;

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

(6) Work 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 Veterans Health Administration (VHA) Handbook 1605.1 and that VA regulations governing the Privacy Act are followed;

(7) Conduct Privacy Act Reviews as described in section 7 of this handbook, per 5 U.S.C. § 552a(e)(1);

(8) Review each SORN biennially to ensure it accurately describes the SOR and certifying to VA Privacy Service that the review was completed;

(9) Prepare new or modified system reports and related documents and ensure that systems of records are not operated without first publishing the required notices and reports; submit each SORN for republication in its entirety every 6 years, regardless of whether there have been any changes to the SOR;

(10) Determine whether the SOR may be exempted from certain provisions of the Privacy Act (5 U.S.C. § 552a(j) and (k)) and take the necessary steps to invoke the exemptions. If the SOR is exempt, the exemption must be reviewed every 3 years to determine if the exemption is still needed;

(11) Ensure a Privacy Act Statement is included on forms (either electronic or paper-based) that collect personally identifiable information (PII), or on separate forms that can be retained by individuals;

(12) Ensure PII is disclosed internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices;

(13) Ensure sharing of PII externally is only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

(14) Keep the SORNs current;

(15) Work with Records Officer to ensure 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; and

(16) Determine with the Privacy Officer or designee the legal authority that permits the collection, use, maintenance and sharing of PII and document the authority to collect PII in the SORN and Privacy Act Statement.

b. **Information System Owner** shall: Ensure that electronic access to information systems under their area of responsibility are in place.

c. **Information Owner/Steward** shall: Ensure the information in the system is accurate, timely, complete, relevant and necessary to accomplish a VA mission.

d. **Records Officer for VA Administrations and Staff Offices** shall: Ensure 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. If 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 SOR may be destroyed until a records schedule is issued by the Archivist.

3. **PUBLISHING SORNs.**

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 SOR. A SORN is comprised of the Federal Register notice(s) that identifies the SOR, 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 SORN**. Agencies must publish a SORN in the Federal Register when establishing a new SOR. They must also publish a notice in the Federal Register when making significant changes to an existing SOR. As a general matter, significant changes are those that are substantive in nature and therefore warrant a revision of the SORN to provide notice to the public of the character of the modified SOR. 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 expanding 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 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 SOR is maintained;

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

(6) A change that modifies how 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 substantially increases the accessibility of the information within the agency;

(8) A new routine use or significant change to an existing routine use that can expand the availability of the information in the system; and

(9) The promulgation of a rule to exempt a SOR from certain provisions of the Privacy Act (a Privacy Act exemption rule that is part of a report of a new or significantly modified SOR 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 SOR would require a revised SORN if the changes are substantive and therefore warrant additional notice. If there are questions about whether particular changes to a SOR are significant, contact VA Privacy Service for assistance.

c. **What to Publish in a SORN**. Each notice of a new or modified SORN shall be drafted using the Office of the Federal Register SORN template, provided in Appendix II to OMB Circular A-108 or by contacting VA Privacy Service at Privacy_Act_Programs. 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 SORN**. The agency responsible for maintaining a SOR (including providing for the operation of a SOR 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 SOR. For a Government-wide SOR, 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 SOR will be maintained by an Administration or Program Office, the System Manager or designee shall work with VA Privacy Service to publish the SORN. VA Privacy Service shall monitor the entire approval process for the SORN, except for VHA, which will be monitored once it has been tasked for final Chief Information Officer (CIO) signature to OIT Front Office. Then, VA Privacy Service will forward the SORN for Congressional and OMB review (where appropriate), forwarding the SORN to the Federal Register for publication once the Congressional and OMB review is completed.

e. **Timing of a SORN**. A new or modified SORN is effective upon publication in the Federal Register, except 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 routine 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's Administration or Program Office that owns the SOR may begin to operate it. VA may collect, maintain and use records in the system. 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 calendar 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.

NOTE: Any reference to 30 days from here forward will refer to calendar days, rather than business days.

(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's Administration or Program office that owns the SOR 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 the System Manager or designee determines that significant changes to the SORN are necessary, the System Manager or designee shall publish a revised SORN. If the System Manager or designee 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 SOR**. When VA stops maintaining a previously established SOR, the System Manager or designee 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 at Privacy_Act_Programs for the template). The notice of rescindment shall identify the SOR, 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 until destruction is permitted per the record retention schedule. If the records in the SOR will be combined with another SOR or maintained as part of a new SOR, 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 its records information about individuals that is relevant and necessary to accomplish a purpose that is required by statute or executive order. If a SOR 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 (NARA).

g. **Format and Style of a SORN**. System Managers or designees 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 SOR. System Managers or designees shall follow the publication format in the Office of the Federal Register SORN templates, provided in the appendices to OMB Circular A-108. In addition, VA shall consult the Office of the Federal Register's Document Drafting Handbook (OFR Handbooks) for general guidance on drafting Federal Register notices.

h. **Scope of a SOR**. The Privacy Act requires agencies to publish a separate SORN for each SOR. Before developing a SORN, VA shall carefully consider the proper scope of the SOR. VA has discretion in determining what constitutes

a SOR for purposes of preparing a notice. However, the System Manager or designee 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. The System Manager or designee 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. The System Manager or designee 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 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, the System Manager or designee 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; and

(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 SOR. 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 SOR 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 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, the System Manager or designee shall explain this linkage in the "Policies and Practices for Retrieval of Records" section of both SORNs.

i. **Government-wide SORs**. A Government-wide SOR is a SOR where one agency has regulatory authority over records in the custody of multiple agencies. 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 concerning the records are carried out uniformly across the Federal Government in accordance with the rules of the responsible agency. For a Government-wide SOR, all agencies – not just the agency with Government-wide responsibilities – are responsible for complying with the SORN's terms 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 SOR 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 several 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 consider the need for a new government-wide SOR.

(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 SOR 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. **SORs Operated by a Contractor.**

(1) When VA provides by contract a SOR on behalf of the agency 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's Administration or Program Office that owns it. The System Manager or designee shall publish a SORN for the system, establish an appropriate routine use to permit disclosure of records to the contractor to operate the system and, to the extent consistent with VA's authority, incorporate enforceable clauses in the contract and statement of work, as outlined in VA Handbook 6500.6, 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) The Senior Agency Official for Privacy (SAOP), Chief Privacy Officer (CPO) or their designee shall review and approve all contracts that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals before award to help evaluate whether a SOR will be established and, if so, to include appropriate clauses in the contract. The SAOP and CPO or their designee 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 defined by the Act as "the use of [a] record for a purpose which is compatible with the purpose for which it was collected" (5 U.S.C. § 552a(b)(3)). To qualify as a routine use, the disclosure must be for a purpose 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 SOR, including the categories of users of the records and the purpose of the use. The System Manager or designee may only establish routine uses for a system by explicitly publishing the routine uses in the relevant SORN. When drafting a SORN, System Managers or designees should contact VA Privacy Service at Privacy Act Programs for an inventory of routine uses as drafted by VA Office of the General Counsel. The System Manager or designee is strongly encouraged to publish all routine uses applicable to a SOR in a single Federal Register notice for that system. However, some agencies choose to publish a separate notice of routine uses that apply 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, the System Manager or designee shall ensure that the routine use section of the SORN indicates which of the separately published routine uses apply to the SOR 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. The System Manager or designee shall describe each routine use with sufficient clarity and specificity to ensure that members of the public unfamiliar with the system or the agency's program can understand the uses to which the records are subject. The

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 SOR should indicate its limited scope.

(3) Before establishing a routine use, VA's Office of General Counsel must determine that VA 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 NARA 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 the System Manager or designee is collecting information as part of a new or modified SOR, 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. The System Manager or designee shall meet all applicable requirements before they begin collecting the information, as outlined in VA Directive and Handbook 6309, Collections of Information. For guidance on whether and how these statutes and OMB policies apply to collection activity, the System Manager or designee shall consult OMB guidance and contact OIRA. If the System Manager or designee asks individuals to supply information that will become part of a SOR, they are

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) The System Manager or designee 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 decide on whether or not to respond.

NOTE: When information is collected over the telephone, the System Manager or designee shall provide a way to 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, the System Manager or designee shall tailor the scope and content of the description to provide the most effective notice to the public. The System Manager or designee 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, the System Manager or designee may provide a plain-language reference to 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 SOR 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 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 SOR**. VA Privacy Service shall report to OMB and Congress any proposal to establish or significantly modify a SOR at least 30 days prior to submitting 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 SOR 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 Privacy Service has questions about the timing of the review, VA Privacy Service shall consult with OIRA (OMB Circular A-108).

(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 Privacy Service may submit a formal written request from the SAOP or CPO to OIRA for an expedited advance review period (see section 4.d. of this handbook for information about expedited review requests).

c. **Illustration of Standard Review Process for Systems of Records.**

NOTE: 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 Privacy Service submits a report to OMB and Congress at least 30 days before the 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	Notices published in the Federal Register after review by OMB and	Day 31

receiving positive notice from OMB that the SORN has passed their review, VA Privacy Service may publish the notice in the Federal Register and solicit comments from the public.	Congress are effective upon publication, except for 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.	
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 the SORN receives public comments, the System Manager or designee shall review the comments to determine whether any changes to the notice are necessary. If the System Manager or designee determines that significant changes are necessary, VA Privacy Service will need to begin the review process again.	Day 61

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

(1) **House of Representatives.** VA's CIO – through VA Privacy Service - shall submit SORNs to the chair and ranking member of the House Committee on Oversight and Government Reform, 2157 Rayburn House Office Building, Washington, DC 20515.

(2) **Senate**. VA's CIO – through VA Privacy Service - shall submit SORNs to the chair and ranking member of the Senate Committee on Homeland Security and Governmental Affairs, 340 Dirksen Senate Office Building, Washington, DC 20510.

(3) **OMB**. VA's CIO – through VA Privacy Service - 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 using ROCIS to submit

reports to OMB, VA Privacy Service shall consult the user manuals available on the ROCIS website or register for the training classes conducted by RISC at GSA headquarters.

e. **Request for Expedited Review of a New or Modified SOR**. Although the System Managers or designees are required to provide adequate advance notice of any proposal to establish or significantly modify a SOR, 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 Privacy Service may submit a formal written request from the SAOP or CPO to OIRA for an expedited OMB review period.

(1) The request shall be included in the transmittal letter that VA Privacy Service 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 Privacy Service's request for expedited review, VA Privacy Service will be allowed to publish the notice in the Federal Register after the expedited OMB review period. When OIRA does not grant VA Privacy Service'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.

f. **Content of the SORN package for a New or Modified SOR**. The SORN package for a new or significantly modified SOR 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:

(b) Be signed by the SAOP or CPO, as delegated by the SAOP;

(c) Contain the name, email address and telephone number of the individual who can best answer questions about the proposed SOR;

(d) Contain VA's assurance that the proposed SOR fully complies with the Privacy Act and OMB policies; and

(e) Contain VA's assurance that the proposed SOR 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 SOR referring to the other materials in the report without

simply restating the information provided in those materials. The narrative statement shall describe the purpose(s) for which the System Manager or designee is establishing or modifying the SOR and explain how the scope of the system is commensurate with the purpose(s) of the system.

(a) Identify the specific authority (statute or executive order) under which the SOR will be maintained. The System Manager or designee shall avoid citing overly general authority; rather, the System Manager or designee shall cite the specific programmatic authority for collecting, maintaining, using and disseminating the information.

(b) An evaluation of the probable or potential effect of the proposal on the privacy of individuals whose information will be maintained in the SOR. If the System Manager or designee has conducted one or more privacy impact assessment(s) concerning information technology that will be used to collect, maintain, or disseminate the information in the SOR, the Privacy Impact Assessment (PIA) will likely provide the information necessary to meet this requirement and may be submitted instead of drafting a separate evaluation.

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

(d) 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 SOR and provide the relevant names, OMB control numbers and expiration dates. If the request for OMB approval of an information collection is pending, the System Manager or designee 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 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 SOR (see definition of a significant change to a SOR, Section 3b).

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

(a) For significantly modified systems, the System Manager or designee 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) These may include a signed Privacy Impact Assessment (PIA) (for new SORNs and SORNs where the PIA is referenced in the Narrative Statement) and a redlined comparison version of the SORN.

(c) The System Manager or designee shall include any other supplementary documents requested by OMB.

g. **Reporting General Changes to Multiple Systems of Records**. When VA makes a general change to its programs or information technology that applies similarly 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 SOR 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. VA has promulgated rules in accordance with the Privacy Act at 38 CFR, § 1.575-1.582.

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 SOR from select provisions of the Privacy Act. If the System Manager or designee wishes to promulgate a rule to exempt a SOR, 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 promulgated VA Privacy Act exemption rules, which are to be published in 38 CFR, § 1.582, 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)).

(a) 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).

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

b. **SORN Revision**. In addition to promulgating a rule, if the System Manager or designee wishes to claim an exemption for a SOR, they shall also identify the applicable exemption(s) in the relevant SORN. Whenever the System Manager or designee publishes a rule to claim a new or revised exemption for a SOR, 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 the System Manager or designee wishes to promulgate a Privacy Act exemption rule, they shall submit the draft rule to OMB along with the new or revised SORN(s) associated with the systems that the System Manager or designee wishes to exempt (see section 4 of this handbook for information about reporting a new or modified SOR). 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 Privacy Service 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 the Act and established OMB 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 SOR for which the exemption is necessary and appropriate. In cases where it is necessary to maintain exempt and non-exempt records in a single SOR, agencies shall only exempt the records for which the exemption is necessary and appropriate.

e. **Reporting and Publication**. The System Manager or designee may not exempt any SOR from any provision of the Privacy Act until all of the applicable reporting and publication requirements have been met.

6. **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 must 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 information systems, VA Privacy Service 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 Privacy Service 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 Privacy Service 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 SOR shall address the following elements:

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

(2) **SORNs**. VA Privacy Service 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 SOR); 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 SOR).

(3) **Routine Uses**. VA Privacy Service 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 Privacy Service shall ensure that each exemption claimed for a SOR 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 Office of Strategic Sourcing 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 Privacy Service shall ensure that its training practices are sufficient and that agency personnel understands the requirements, OMB guidance, VA's implementing regulations and policies and any job-specific requirements.

c. **VA Privacy Act Reviews**. To comply with the requirements of the Privacy Act and OMB guidance, VA Privacy Service will conduct a review of each SORN every three years. The System Manager or designee will complete the review and return a signed checklist to VA Privacy Service. If there have been significant changes, the System Manager or designee will prepare the documents to republish the SORN in its entirety. If the system is obsolete, the System Manager or designee will prepare a rescindment SORN. Every 6 years, the System Manager or designee 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 and CPO.

7. **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. 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.

8. **AGENCY WEBSITE POSTING.** VA Privacy Service shall maintain a central resource page dedicated to its privacy program on its principal website at VA Privacy Service. At a minimum, VA Privacy Service shall include the following materials related to the Privacy Act on its central privacy program page:

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

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

(2) Citations and links to all Federal Register notices that comprise the SORN for each SOR; and

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

NOTE: The requirement for VA Privacy Service to provide links to complete, up-to-date versions of SORNs on VA's privacy program page does not replace the Privacy Act's statutory requirement for VA Privacy Service to publish SORNs in the Federal Register. Notice in the Federal Register a SOR 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 Privacy Service 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 Privacy Service shall list and provide links to all VA 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 Privacy Service shall provide references for individuals who wish to request access to or amend their records pursuant to 5 U.S.C. § 552a(d).

9. **VA PRIVACY SERVICE CONTACT INFORMATION**

a. Hotline: 202-273-5070

b. Mailbox: privacy_act_programs@va.gov

10. **DEFINITIONS**

a. **Disclosure**. Release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information (SOURCE:42 U.S.C. §§ 1320d-d-8; 264(3)).

b. **Individual**. A citizen of the United States or an alien lawfully admitted for permanent residence (SOURCE: 5 U.S.C. § 552a). NOTE: The definition of "individual" under the Privacy Act differs from the definition of "individual" under the Freedom of Information Act (FOIA). Deceased persons, non-resident aliens, businesses and organizations are not "individuals" under the Privacy Act.

c. **Maintain**. To collect, use, or disseminate (SOURCE: 5 U.S.C. § 552a).

d. **Privacy Act Statement.** Agencies are required to provide what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security Number) (SOURCE: 5 U.S.C. § 552a(e)(3)).

e. **Privacy Impact Assessment (PIA)**. A PIA is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy concerns. A PIA is both an analysis and a formal document detailing the process and the analysis outcome (SOURCE: OMB Circular A-130).

f. **Record**. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, their education, financial transactions, medical history and criminal or employment history and that contains their name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph (SOURCE: 5 U.S.C. § 552a).

g. **Routine use**. With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected (SOURCE: 5 U.S.C. § 552a).

h. **System of records (SOR)**. A group of any records under the control of any agency from which information is retrieved by the name of the individual or identifying number, symbol, or other identifying particular assigned to the individual (SOURCE: 5 U.S.C. § 552a, NIST 800-122).

i. **System of records notice (SORN)**. The notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a SOR describing the existence and character of the system. A SORN identifies the SOR, 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 (SOURCE: OMB Circular A-108).

11. **REFERENCES**.

a. E-Government Act of 2002, Pub. L. 107-347, Section 208.

b. Federal Information Security Modernization Act of 2014, Pub. L. 113-283.

c. Freedom of Information Act (FOIA), 5 U.S.C. § 552, 38 CFR §§ 1.550-557 (1967).

d. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, 42 U.S.C. §§ 1320d-d-8; 264(3).

e. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Administrative Regulations, 45 CFR Parts 160 and 164.

f. National Institute for Standards and Technology Special Publication 800-37, Revision 2, Risk Management Framework for Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018.

g. National Institute for Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of PII, April 2010.

h. National Institute for Standards and Technology. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0, January 16, 2020.

i. OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act, December 23, 2016.

j. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, July 27, 2016.

k. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, July 27, 2016.

l. OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

m. OMB M-05-08, Designation of Senior Agency Official for Privacy, February 11, 2005.

n. OMB M-06-15, Safeguarding PII, May 22, 2006.

o. OMB M-06-16, Protection of Sensitive Agency Information, June 23, 2006.

p. OMB M-16-24. Role and Designation of Senior Agency Officials for Privacy. September 5, 2016.

q. Paperwork Reduction Act of 1995, 44 U.S.C. § 3501 et seq.

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

s. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, August 19, 2013.

t. VA Directive 6309, Collections of Information, January 12, 2010.

u. VA Handbook 6309, Collections of Information, January 12, 2010.

v. VA Directive 6502, VA Enterprise Privacy Program, May 5, 2008.

w. VA Handbook 6502.4, Procedures for Computer Matching Programs, August 22, 2018.

x. VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program, February 24, 2021.

y. VA Handbook 6500.6, Contract Security, March 12, 2010.

z. VA Directive 6508, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014.

APPENDIX - VA SORN APPROVAL PROCESS

1. Before beginning the SORN process for a new collection of records, check to see if there is an approved SORN that is appropriate in scope and can be amended. If there is none, check to see if there is an approved Privacy Impact Assessment (PIA) for the IT system being used to collect the records. Refer to VA Directive 6508 located at: http://www.va.gov/vapubs. Contact PIA Support at PIASupport@va.gov for PIA assistance.

2. Once you determine there is a current PIA for the IT system being used to collect the records, you may begin the SORN process to create a new or amend a SORN. You may contact VA's Privacy Service at (202) 273-5070, or by email to Privacy_Act_Programs@va.gov to coordinate SORN efforts. The same process is used, regardless of VA Administration, with the exception of VHA, which may be contacted at the VHA Privacy Office by e-mail at VHA105HIGPrivacyBRATeam@va.gov.

   a. **Step 1**. If it is a new SORN, contact VA Privacy Service (005P1A) to receive a 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). There is no limit on how many characters the SOR number can have. If it is a modified SORN, use the existing SOR number – however, you may change the mail routing symbol.

   b. **Step 2**. Draft the appropriate documents (see table on the next page). Contact VA Privacy Service for templates. Note that only new SORNs and those that modify routine uses are subject to OMB and congressional review and public comment.

   c. **Step 3**. Create a SORN submission package in VA's Integrated Enterprise Workflow System (VIEWS), load the documents to the "Documents" tab and make assignments to the appropriate offices for concurrence on the Concurrence and Summary Sheet (VA Form 4265).

	New SORN	Significantly modified SORN or routine uses	Not significantly modified nor changes to 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 4.e.(1) of this handbook)	Yes	Yes	No	No
Narrative Statement, including information from the privacy impact assessment (see section 4.e.(2))	Yes	Yes	No	No
Exemption Rule (see section 4.e.(4))	Yes, if applicable	Yes, if applicable	No	No
Supplementary Documents, including a marked-up version of previous SORN (see section 4.e.(5))	Yes, if applicable	Yes	No	No
Concurrences from Administration or Program Office per internal policy	Yes	Yes	Yes	Yes
Additional Concurrences	OCLA (009)" OGC (02)""	OCLA (009) OGC (02)	OGC (02)	OCLA (009) OGC (02)

*OCLA – Office of Congressional and Legislative Affairs

**OGC – Office of General Counsel

d. **Step 4**. Once the concurrences are obtained, make an assignment in VA's correspondence control system to OIT Front Office (005) for review and concurrence. VA Privacy Service will review all SORN packages and recommends approval, as appropriate, to the SAOP or CPO.

e. **Step 5**. The SAOP or CPO approves the package and signs the SORN and/or letters.

f. **Step 6.** VA Privacy Service uploads the signed SORN and related documents into ROCIS and submits the package electronically to OMB. VA Privacy Service also submits the packages to OCLA for dispatch to a member of Congress.

g. **Step 7**. For new SORNs or significantly modified SORNs, OMB and members of Congress have 30 days to review and comment (VA Privacy Service must wait for OMB clearance, which may take longer than 30 days). 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 send them to the originator of the SORN, who must review and determine if revisions to the SORN are warranted.

h. **Step 8**. Once the SORN is published, it will be posted to VA's Internet site, http://www.va.gov/privacy by VA Privacy Service.