Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6502.3
Transmittal Sheet
June 3, 2011

WEBPAGE PRIVACY POLICY

1. REASON FOR ISSUE: To revise the Department of Veterans Affairs (VA) agency-wide procedures that implement the policies contained in VA Directive 6502.3, Web Page Privacy Policy, for creating privacy policies for VA Internet Web pages and implementing the policies set forth in VA Directive 6502, Privacy Program.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This handbook provides procedures for implementing the privacy policy provisions of the E-Government Act of 2002, as well as relevant Office of Management and Budget (OMB) guidance relating to the posting of privacy policies on federal Web pages.

3. RESPONSIBLE OFFICE: Office of Information and Technology (005), Office of Information Security (005R), Office of Privacy and Records Management (005R1).

4. RELATED DIRECTIVE: VA Directive 6502.3, Web Page Privacy Policy.

5. RESCISSIONS: VA Handbook 6502.3, Web Page Privacy Policy, dated April 17, 2006.

CERTIFIED BY:

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

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

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

Distribution: Electronic

WEB PAGE PRIVACY POLICY

CONTENTS

WEB PAGE PRIVACY POLICY

1. PURPOSE AND SCOPE

a. This document outlines general guidelines with regard to creating, posting, and maintaining all Department of Veterans Affairs (VA) Web page privacy policies on the Internet.

b. The requirements in this document do not extend to non-public VA intranet pages.

c. While the term “privacy statement” is frequently used, current Office of Management and Budget (OMB) Guidance requires that to promote clarity for the public, all Federal agencies must use the term “privacy policy” when referring to their posted policy statements relating to Web page privacy.

d. This handbook provides guidance and describes requirements regarding both the policy applicable to all VA Web pages (the VA General Web Privacy Policy, or “the general policy”), and policies limited in scope to a particular Web page or set of Web pages. (Limited Web Privacy Policies, or “limited policies”).

e. The term “privacy policy” applies to both general and limited policies.

f. In order to promote compliance with existing Federal privacy laws, regulations, and guidance, this handbook provides procedures and requirements to those individuals who are responsible for the development and maintenance of VA Web pages.

g. This handbook is not limited to any specific technology or application and it includes VA’s use of third-party Web measurement and customization technologies.

h. Whenever third-party Websites or applications are used to engage with the public, the hosting office must refer to OMB’s memorandum M 10-23, *Guidance for Agency Use of Third-Party Websites and Applications*.

i. In some cases, the third-party Websites or applications use Web measurement and customization technologies solely for the third-party’s own purposes. Service of VA cookies through third-party Websites and applications (TPWA) is never permitted. This policy does not apply as long as:

(1) Third-parties do not use Web measurement and customization technologies on behalf of a Federal agency; and

(2) Personally-Identifiable Information (PII), or any information that could be used to determine an individual’s online activity derived from such uses, is not shared with VA;

j. Cookies of TPWA must be evaluated to ensure that they are clearly performing according to their tier designation.

2. REQUIREMENTS AND PROCEDURES

a. **General Considerations.**

(1) All VA Web privacy policies should be clear, concise, and written in plain language.

(2) Every VA Web page must link to an appropriate privacy policy. For each page, the responsible official (i.e., the page owner) should determine whether a link to the general policy is sufficient to satisfy legal and regulatory requirements, or whether a link to a page-specific or site-specific limited policy is required. This handbook provides additional guidance for making this determination.

b. **The VA General Web Page Privacy Policy.**

(1) The principal VA Web entry page (www.va.gov) and all other Web pages that do not include a link to a limited policy must include a link to the general policy.

(2) The general policy will be updated from time to time as necessary to ensure that it remains accurate and complete to the extent required by applicable law, regulation, or guidance. Thus, Web pages must link to the version of the policy maintained by the Privacy Service (005R1A) at www.va.gov/privacy , rather than copy the text of the policy and include it on a discrete page.

c. **Limited Web Page Privacy Policies.**

(1) Limited policies must be created, posted, and linked from a particular Web page if:

(a) information collected on that Web page is subject to the Privacy Act of 1974;

(b) applicable law, regulation, or guidance requires that additional privacy policy information be disclosed beyond that included in the general policy; or

(c) Web pages use persistent cookies or Web beacons.

(2) Each limited policy must include a link to the general policy.

(3) A copy of each limited policy must be accessible in a *machine-readable format*, as defined in VA Directive 6502.3 paragraph 5b.

(4) If a particular Web page or set of Web pages collects information subject to the Privacy Act, then the limited policy covering that page must include a Privacy Act Statement, as outlined in Appendix A – Limited Privacy Policy Sample. The Privacy Act Statement must describe:

(a) the authority (whether granted by statute, or by Executive Order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

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

(c) the routine uses which may be made of the information, as published pursuant to the Privacy Act;

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

(e) contact information by which a user may contact the appropriate office for additional information regarding the policy.

(5) If a social security number is being collected, the data subject must be informed whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it.

(6) All limited policies must comply with the requirements of the Paperwork Reduction Act of 1995, as amended, pursuant to VA Directive 6300, Records and Information Management, and related handbooks.

(7) All limited policies must comply with the requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). This Act requires that when VA develops, procures, maintains, or uses electronic and information technology, Federal employees and members of the public with disabilities have access to and use of information and data that is comparable to that provided to individuals without disabilities, unless an undue burden would be imposed on the agency.

(8) Web pages requiring limited policies may be subject to the Privacy Impact Assessment (PIA) requirements of Section 208 of the E-Government Act of 2002 (Pub. L. 107-347). Webmasters and other responsible officials should refer to OMB Memoranda 03-22 and 10-23, and VA Directive 6508, Privacy Impact Assessments and VA Handbook 6508.1, Privacy Impact Assessments for further guidance.

(9) The Webmaster or other responsible official must verify that all collections of PII are protected by appropriate security measures, conforming to the representations made in the limited policy.

d. **Format Requirements for Privacy Policy Links**

(1) Links to privacy policies must be clear and conspicuous. The text of the link must read “Privacy Policy.”

(2) Links to limited policies should be visible on the same screen (viewed at a standard resolution) as the form or email link by which information is collected.

e. **Restrictions on Tracking and Customization Activity.**

(1) Subject to the limitations described below, VA entities may use Web measurement and customization technologies for the purpose of improving online services through conducting measurement and analysis of usage or through customization of the user's experience. However, under no circumstances may any VA entity use such technologies:

(a) to track user individual-level activity on the Internet outside of the Website or application from which the technology originates;

(b) to share the data obtained through such technologies with other departments or agencies, without the user's explicit consent;

(c) to cross-reference any data gathered from Web measurement and customization technologies against PII to determine individual-level online activity, without the user's explicit consent;

(d) to collect PII in any fashion without the user's explicit consent; or

(e) for any like usages so designated by OMB.

(2) Below are the defined tiers for authorized use of Web measurement and customization technologies:

(a) Tier 1 – single-session**.** This tier encompasses any use of single-session Web measurement and customization technologies.

(b) Tier 2 – multi-session without PII. This tier encompasses any use of multi-session Web measurement and customization technologies when no PII is collected (including when VA is unable to identify an individual as a result of its use of such technologies).

(c) Tier 3 – multi-session with PII. This tier encompasses any use of multi-session Web measurement and customization technologies when PII is collected (including when VA is able to identify an individual as a result of its use of such technologies).

f. **Clear Notice and Personal Choice.** VA entities must not use Web measurement and customization technologies that make it difficult for the public to opt-out. In order to use Web measurement and customization technologies, the entity must explain how the user will be affected by opting-in or opting-out of use of the measurement or customization technology. VA entities must provide users who decline to opt-in or decide to opt-out with access to information that is comparable to the information available to users who opt-in or decline to opt-out.

(1) **VA Opt-out.** VA entities are encouraged, where appropriate, to use Web tracking and measurement technologies in order to remember that a user has opted-**out** of all other uses of such technologies on the relevant domain or application. Such uses of tracking and measurement technologies are considered Tier 2.

(2) **Client side opt-out.** Where client-side opt-out is possible, the mechanism used to opt-out should be as simple as possible. If opt-out mechanisms are not appropriate or available, instructions on how to enable client side opt-out mechanisms may be used. Client side opt-out mechanisms allow the user to opt-out of Web measurement and customization technologies by changing the settings of a specific application or program on the user's local computer. For example, users may be able to disable persistent cookies by changing the settings on commonly used Web browsers. For further guidance, the entity creating the Website should refer to http://www.usa.gov/optout_instructions.shtml. This Website contains general instructions on how the public can opt-out of some of the most commonly used Web measurement and customization technologies.

(3) **Tier 3 restrictions.** VA entities employing Tier 3 uses of measurement and customization technologies must only use opt-in functionality.

g. Data Safeguarding and Privacy.

(1) All uses of Web measurement and customization technologies must comply with existing policies with respect to privacy and data safeguarding standards. If applicable, the appropriate PIA and/or System of Records Notice (SORN) must be cited in the online privacy policy.

(2) All VA entities using Web measurement and customization technologies in a manner subject to Tier 1 or Tier 2 are authorized to use such technologies so long as those entities:

(a) Are in compliance with this handbook and all other relevant policies;

(b) Provide clear and conspicuous notice in their online privacy policy citing the use of such technologies, as specified in Appendix A; and

(c) Comply with their internal policies governing the use of such technologies

h. **Privacy Review.**

(1) Any proposals to engage in Tier 3 uses must be reviewed by the VA Privacy Service.

(2) A PIA is required whenever a TPWA makes PII available to VA. A SORN is required if the information collected is kept in a System of Records as defined by the Privacy Act of 1974.

(3) The VA Privacy Service shall provide a PIA template specifically tailored for TPWA sites. This PIA will address functions specific to TPWA sites. Multiple TPWA uses may be authorized under a single PIA so long as the PIA relates to a single TPWA and all practices in which VA engages are subject to the same agreement.

(4) If any use of a TPWA raises a distinct privacy risk, a separate PIA is required. A separate PIA is required even if there is an existing PIA for the TPWA. TPWA PIAs, at minimum, will ask the following questions:

(a) The specific purpose of the use of the TPWA;

(b) Any PII that is likely to become available to VA through the public use of the TPWA;

(c) The activity's intended or expected use of any PII (e.g., to identify users and/or communicate with them);

(d) With whom any PII that is collected will be shared;

(e) Whether and how the activity will maintain PII and for how long;

(f) Whether and how the agency will maintain, use, or share PII that becomes available through the use of the TPWA (all uses and potential sharing of information should be considered and disclosed);

(g) How the activity will secure PII that it uses or maintains;

(h) What other privacy risks there are and how the activity will mitigate those risks;

(i) Whether the activity will create or modify an existing System of Records under the Privacy Act of 1974;

(j) Whether sufficient due diligence has been conducted on the TPWA privacy policy in order to ensure that there the level of risk involved with using the TPWA is acceptable; and

(k) If a link is posted to a TPWA, whether it provides a warning that the user is being directed to a non-government site, and provide an explanation of the risk involved with providing PII.

i. **Notice and Comment.**

(1) PIAs for the use of Tier 3 multi-session cookies must be submitted to the VA Privacy Service (005R1A) for review and approval. Following Privacy Service review and approval, the requesting office must:

(a) Solicit comment through the VA Open Government Webpage at www.va.gov/open for a minimum of 30 days. This notice must include the proposal to use such technologies and a description of how the technology will be used. The notice should, at a minimum, address the items in the privacy policy as described in Appendix A; and

(b) Review and consider substantive comments and make changes to their intended use of Web measurement and customization technologies where appropriate.

(2) With written approval from the VA Chief Information Officer (CIO), VA entities are exempt from this requirement if the notice-and-comment process is reasonably likely to result in serious public harm.

j. **Tier 3 Review.** All VA entities using Web measurement and customization technologies in a manner subject to Tier 3 must have explicit written approval from the VA CIO or his or her

designee. This approval must be cited in the online privacy policy. After this approval has been obtained and after notice and comment, as specified in paragraph 2(i), has been completed, the entities are authorized to use Tier 3 Web measurement and customization technologies.

k. **Previous Authorization for Use of Web Measurement and Customization Technologies.** Waivers will not be granted to sites that were previously granted authorizations. Those sites must bring their operations into compliance with this handbook.

l. **Unauthorized Use.** If any VA Website is found to be using Web measurement and customization technologies outside of the process or parameters specified in this policy, the responsible office must inform the VA CIO and OMB of the extent of any unauthorized use. The VA CIO and OMB will respond as necessary and appropriate.

m. **Comparable information and Services.** If any activity is using a Website or application hosted on a third-party site using Web measurement and customization technologies to which Federal privacy and data safeguarding standards do not apply, they should provide the public with alternatives for acquiring comparable information and services. For example, members of the public should be able to learn about the activity or to communicate with the responsible office without having to join a third-party social media Website. If the third-party service is used to solicit feedback, the responsible office should provide an alternative government email address where users can also send feedback.

n. **Data Retention Limits and Access Limits.** VA offices may retain data collected from Web measurement and customization technologies for only as long as necessary to achieve the specific objective for which it was collected. Moreover, only employees who need to have access to the data should be allowed to do so.

(1) **Retention time.** The time frame for retention of data must be both limited and correlated to a specific objective. If not required by any record retention schedule, some other law, policy, or a specific need for the Web measurement or customization objective, such data should be retained for one year or less.

(2) **Records disposition schedule.** Information collected from Web measurement and customization technologies that is determined to be a Federal Record must comply with Federal Records Act regulations. General Records Schedule 20 (GRS 20) pertains to Electronic Records; specifically, the disposition authority cited in General Record Schedule 20 Item 1C, "Electronic Records" ("*Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records - Electronic files … created to monitor system usage*…") is applicable to information collected from Web measurement and customization technologies. Use of GRS 20 is mandatory for those categories of electronic records described in the schedule unless the agencies have requested an alternative disposition authority from the National Archives and Records Administration**.**

o. **Enforcement.** To the extent feasible, technical enforcement mechanisms should be put in place to implement stated retention times and to limit access to authorized personnel.

Where technical enforcement mechanisms are not feasible, policy or contractual enforcement mechanisms must be present.

p. **Verification.** VA entities using Web measurement and customization technology must annually review their systems and procedures to demonstrate that they are in compliance with this policy. All reviews of Tier 3 uses must be submitted to the VA Privacy Service for approval. The results of these reviews and approvals shall be posted on the VA open government page.

3. DEFINITIONS

a**. Multi-session technologies**. These technologies remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier (i.e., cookie) for each user, which lasts across multiple sessions or visits.

b. **Personally-Identifiable Information (PII).** A subcategory of VA Sensitive Data, PII means any information about the individual maintained by an agency, including but not limited to the following: (1) education, financial transactions, medical history, and criminal or employment history; (2) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records or any other personal information which is linked or linkable to an individual.

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

d. **Single-session technologies.** These technologies remember a user's online interactions within a single-session or visit. Any identifier correlated to a particular user is used only within that session, is not later reused, and is deleted immediately after the session ends.

e. **Third-Party Websites and Applications (TPWA).** Web-based technologies that are not exclusively operated or controlled by a VA entity. This includes non .gov hosted applications and applications that can be embedded on a government Webpage. Examples include embedded YouTube videos or links to Facebook.

f. **Web measurement and customization technologies.** These technologies are used to remember a user's online interactions with a Website or online application in order to conduct measurement and analysis of usage or to customize the user's experience.

DEPARTMENT OF VETERANS AFFAIRS LIMITED PRIVACY POLICY SAMPLE

This limited policy applies only to the following Web page(s): [URL]. For general information regarding the information handling policy of the Department of Veterans Affairs (VA), please review the Department of Veterans Affairs general Web privacy policy, available at www.va.gov/privacy .

Privacy Act Statement

VA follows the requirements of the Privacy Act, which protects your personal information that we maintain in what are called systems of records. A system of records is a file, database, or program from which personal information is retrieved by name or other personal identifier. In other words, the Privacy Act applies when we use your personal information to know who you are and to interact with you – such as when you provide information to request a product or service, register on one of our Websites, or submit an inquiry or complaint. The Privacy Act provides a number of protections for your personal information. This includes how information is collected, used, disclosed, stored, and discarded.

The Web page from which you linked to this limited policy [URL] collects certain information from you which may be subject to the Privacy Act. This information includes:[describe information collected – state purposes and state routine uses].

VA publishes notices in the Federal Register that describe in more detail when information about you may be made available to others. A copy of the notice(s) and any relevant amendments relating to [URL] is available at the following locations:

[URL for SOR Notice] *[Note that link must go directly to RELEVANT SOR Notices.]*

[If not stated in the SOR Notice, state:] The collection of information on [URL] is authorized by [cite authority]. Your disclosure of such information is voluntary.

The principal purpose(s) for which the information will be used is [state purpose or purposes].

By voluntarily providing information on [URL], you are consenting to VA's use and disclosure of that information in the manner described in this limited policy, the Department of Veterans Affairs general Web privacy policy, and the Privacy Act notice to which a link is provided above. If you refuse to provide this information, [state effects, e.g., inability to apply for benefits electronically, VA will be unable to process your request, etc. Description must be specific, i.e., it must describe effects of not providing all or any part of requested information.] However, refusal to provide this information will not prevent you from accessing comparable information or services.

Additional information regarding your legal rights is available at: [provide link to a Privacy Act rights summary and a FOIA rights summary].

Tracking and Site Measurement and Customization Technologies

[Describe and state authority, if required.

Web measurement and customization technologies are used on this site in order to [cite the purpose of the Web measurement technology.] This use is considered a [cite tier] technology and it is [site session type (e.g., persistent or single session)] that uses [state the type of technology used]. This technology is used to collect information under the authority of [state legal authority]. This technology will be used to collect information related to [cite the nature of the information collected]. This information will be used to [cite the purpose and use of information] and it [will/will not] be disclosed [state to whom it will be disclosed, if anyone]. The measures taken to protect his information from unauthorized use include [state the privacy safeguards applied to the information]. This data will be retained for a period not to exceed [state the data retention policy]. This [state the customization technology type] [will/will not] be enabled by default. You may opt out of the use of this [state measurement/customization technology type]. If you would like to opt out of the use of this [state customization technology type], you must [state how to opt out of the Web measurement/customization technology]. Please note that opting out of the use of this [state the type of Web measurement/customization technology] will not prevent you from accessing comparable information or services. This [state customization technology type] was provided through the cooperation of the Department of Veterans Affairs and [name all third party vendors].

Information Collected from Online Forms

Many of our programs and Websites allow you to send us an email. Generally, we will use the information you provide to respond to your inquiry. In some circumstances VA may be required by law to retain or forward emails; examples of such emails might include emails that contain threats to VA personnel or property or contain information that is required as part of a judicial proceeding. Remember that email may not be secure against interception. If your email communication is very sensitive, or includes information such as your bank account, charge card, or social security number, you should send it by mail unless the Website clearly indicates that such communications are appropriately secured.

Security

In those instances where we secure your personal information in transit to us and upon receipt, VA uses Federal Information Processing Standards (FIPS) 140-2 validated encryption. The URL in your browser will change to “HTTPS” instead of “HTTP” when this security feature is invoked. Your browser may also display a lock symbol on its bottom task bar line to indicate this secure transmission is in place.

For site security purposes and to ensure that VA Websites remain available to all users, VA employs software programs to monitor network traffic in order to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law

enforcement investigations, no other attempts are made to identify individual users or their usage habits other than those uses identified in this policy. Unauthorized modification or misuse of information stored on VA systems will be investigated and may result in criminal prosecution. VA takes the security of all personally identifiable information we maintain very seriously. We implement various measures to protect the security and confidentiality of personally identifiable information. Such measures include access controls designed to limit access to personally identifiable information to the extent necessary to accomplish our mission.

We also employ various security technologies to protect personally identifiable data stored on our systems. We test our security measures periodically to ensure that they remain operational.

Information from Children [Include Only if Collecting Information from Children Under 13]

VA may, from time to time, collect information from children under 13 years of age. In instances where we collect personal information from children under 13 years old, we will do so only with parental notice and consent. We will take reasonable steps necessary to protect the privacy and safety of any child from whom information is collected, in accordance with the Children's Online Privacy Protection Act (COPPA).

Contact Information
For additional information regarding this limited policy please contact:
[Insert Contact info.]