Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6502.3
Transmittal Sheet
April 17, 2006

WEB PAGE PRIVACY POLICY

1. REASON FOR ISSUE: To establish policy for the Department of Veterans Affairs (VA) for the publication and maintenance of Privacy Policies covering all VA Web pages available to the public.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: The directive sets forth:

a. This policy requires that all VA Web pages post Privacy Policies, as required by VA directives and in accordance with applicable laws, regulations, and administrative guidance, and defines the organizational responsibilities for the posting of Privacy Policies on VA Web pages. This policy also describes the required content of Privacy Policies and establishes the organizational responsibilities associated with the development and maintenance of such Privacy Policies.

b. This policy complies with OMB Memoranda 99-18, *Privacy Policies on Federal Web Sites*, and 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. This policy also complies with the E-Government Act of 2002, which requires that all federal Web pages make certain disclosures to users via a posted privacy policy, and the Privacy Act of 1974, as amended, which requires additional disclosures under certain circumstances.

3. RESPONSIBLE OFFICE: Office of Policy, Portfolio Oversight & Execution (005P), Office of the Assistant Secretary for Information and Technology (005).

4. RELATED HANDBOOK: VA Handbook 6502.3; Web Page Privacy Policy.

5. RESCISSIONS: None

CERTIFIED BY:

/s/

Robert N. McFarland
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Robert N. McFarland
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

Blank

WEB PAGE PRIVACY POLICY

1. PURPOSE AND SCOPE

a. This directive mandates the creation of a VA General Web page Privacy Policy (the General Policy), setting forth how information collected via VA Web sites, pages, and forms is to be collected, used and maintained. This directive establishes the requirements and responsibilities for the creation and maintenance of Limited Privacy Policies (Limited Policies), which govern the handling of personally identifiable information collected via specific Web sites, pages, and forms. This directive also designates the officials responsible for the General Policy and Limited Policies.

b. The directive applies to all individuals supporting VA Web sites, including but not limited to full-time and part-time employees, contractors, interns, and volunteers.

c. This directive only applies to government information as defined in OMB Circular A-130, i.e., information created, collected, maintained, processed, disseminated, or disposed of by or for the Federal Government.

2. POLICY

a. Privacy Policies

(1) All VA privacy policies must 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(s) (individual(s) responsible for the creation, design, maintenance, or deployment of a VA Web page) must determine whether a link to the General Policy is sufficient to satisfy legal and regulatory requirements, or whether a link to a page- or site-specific Limited Policy is required.

(3) All VA privacy policies must include contact information by which a user may contact the appropriate office for additional information regarding the policy.

b. General Web Page Privacy Policy

(1) The General Policy is maintained and updated by the VA Privacy Service. The current version is available at www.va.gov/privacy.

(2) The General Policy must be updated as necessary to ensure that it remains accurate and complete to the extent required by applicable law, regulation, or guidance.

(3) The format of the General Policy must, at a minimum, include the following paragraphs:

(a) Introductory language.

(b) Information collected and stored automatically.

(c) Information collected from Web forms.

(d) Security, intrusion, and detection language.

(e) Significant actions where information may be subject to the Privacy Act.

(4) The General Policy must address the following requirements:

(a) Notice of Limited Policies. The General Policy must advise users that Limited Policies will be posted on any pages where additional legal or regulatory disclosure requirements apply, provide the Privacy Act Statement applicable to such pages, and encourage users to review the privacy policy linked to any Web page prior to submitting information via that page.

(b) Nature, purpose, use, and sharing of information collected. The General Policy will direct users to Limited Policies for specific information about the nature, purpose, use, and sharing of specific information collected on such pages.

(c) Privacy Act information. The General Policy will direct users to Limited Policies for information regarding the collection of information subject to the Privacy Act on such pages.

(d) Tracking and customization activities. The General Policy will restrict the use of tracking and customization activities as required by applicable law and OMB guidance.

(e) Law enforcement sharing. The General Policy shall reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security, and national security activities.

(f) Automatically Collected Information. The General Policy must generally state what information VA Web sites collect automatically (i.e., user's IP address, location, and time of visit) and identify the purpose for which it is collected (i.e., site management or security purposes).

(g) Intentional Interaction with children. The General Policy must include a statement satisfying the requirements of the Children's Online Privacy Protection Act of 1998 (COPPA).

(h) Additional legal requirements. The General Policy shall state that, whenever required by law, additional disclosure requirements under specific statutes and their implementing regulations must be satisfied in the appropriate Limited Policy.

(5) A copy of the General Policy must be accessible in a *machine-readable format*, as defined in 5.b.

c. Limited Privacy Policies

(1) Every Web site that collects information from users that is subject to additional legal or regulatory requirements beyond those stated in the General Policy must include a link to an appropriate Limited Policy.

(2) Each Limited Policy must clearly specify its scope and its relationship to the General Policy, and must clearly and conspicuously link to the General Policy.

(3) Limited Policies must provide any additional information required by law, regulation, or applicable guidance regarding the maintenance and use of information collected via a specific Web page. Such information will include, where required:

(a) Information regarding consent to collection and sharing of data,

(b) Privacy Act Statements. Privacy Act Statements must notify users of:

1. the authority for, purposes and routine uses of the collection of information subject to the Privacy Act,

2. whether providing the information is mandatory or voluntary,

3. the effects of not providing all or any part of the requested information, and

4. if a social security number is being collected, the data subject must be specifically informed whether that disclosure is mandatory, voluntary or required to retain or obtain benefits, by what statutory authority such number is solicited, and what uses will be made of it.

(c) Additional legal requirements. If additional disclosures are required under applicable law, regulation, or guidance, (e.g., Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act of 1999, etc.) and such disclosures are not made on the page where information is collected, than such disclosures must be made in the Limited Policy. If such disclosures are made on the page, the Limited Policy must reference the additional requirements and when practical link to these requirements.

3. RESPONSIBILITIES

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

(1) Establish Department-wide requirements, and provide oversight and guidance for all VA Web page privacy issues;

(2) Designate the Associate Deputy Assistant Secretary (ADAS) for Policies, Plans and Programs, as the principal Department official responsible for the VA Privacy Program;

(3) Provide oversight and review of the privacy protection of data used and collected on VA Web pages as required by applicable law, regulation and guidance.

b. The Associate Deputy Assistant Secretary (ADAS) for Policy, Portfolio Oversight & Execution. The ADAS shall:

(1) Provide for the development, issuance and monitoring of Web page Privacy Policies, in accordance with applicable Federal law and guidance;

(2) Facilitate cooperation among all Under Secretaries, Assistant Secretaries, and Other Key Officials for the purpose of Web page-related Privacy Policy development and implementation; and

(3) Advise the VA CIO, Under Secretaries, Assistant Secretaries, and Other Key Officials on Web page privacy policy compliance and other issues related to the protection of data collected from and resulting from the use of VA Web pages.

c. Director, Privacy Service. The Director, Privacy Service shall:

(1) Develop, post, and maintain the General Policy;

(2) Coordinate Department-wide Web page privacy requirements, and provide information and guidance in coordination with the Office of General Counsel regarding compliance with all Federal privacy law, regulations, and guidance as applicable to all VA Web pages;

(3) Provide a current user manual that delivers guidance for bringing all Department of Veterans Affairs web pages into compliance with Federal and VA web page privacy policies;

(4) Provide all required Department-wide Web page privacy-related reporting, including recommendations to the ADAS for Policies, Plans and Programs and the CIO as required by applicable law, regulation and guidance; and

(5) Analyze legislative, regulatory, or guidance proposals, in draft or final form, in conjunction with the Office of General Counsel, to determine actual or potential impacts of such measures on VA Web page privacy policy and/or practice.

d. Web Masters or other Responsible Officials. Any individual responsible for the creation, design, maintenance, or deployment of a VA Web site must:

(1) Determine whether each Web page for which he or she is responsible requires a Limited Policy specific to that page;

(2) Consult with the Office of General Counsel and/or the Privacy Service as necessary, and

(3) Post all required Privacy Policies, and confirm that they are appropriately accessible to Web page visitors.

e. Staff Office and Administration Privacy Officers. The Privacy Officer must review the Limited Policies to be posted on Web pages for the Staff Office or Administration

f. The Inspector General. This Office may be requested to:

(1) Conduct and supervise Web page privacy audits, and provide follow-up regarding Web page Privacy Program audit findings; and

(2) Nothing in this Directive shall prevent or impede the Inspector General from performing duties pursuant to the Inspector General Act or other statutory authority.

g. The General Counsel. This Office shall:

(1) Interpret laws, regulations, guidance, and directives applicable to VA Web page privacy issues; and

(2) Upon request, render legal opinions regarding compliance with the Web page privacy laws regulations, guidance, and directives as well as:

(a) Provide legal reviews of audits for compliance with applicable laws, regulations, guidance, and directives; and

(b) Provide legal advice and services to the Secretary, Under Secretaries, Assistant Secretaries, and Other Key Officials related to Web page privacy issues.

h. Under Secretaries, Assistant Secretaries, and Other Key Officials. Under Secretaries, Assistant Secretaries, and Other Key Officials shall:

(1) Ensure, per this directive and other applicable guidance, that Department-wide Web page privacy policies and procedures are implemented;

(2) Ensure that all data (collected via Web pages) within the systems and resources for which they are responsible are adequately secured;

(3) Ensure that all employees and other authorized individuals under their jurisdiction act in compliance with the Department's Web page privacy policies;

(4) Ensure that any reporting or notice requirements are met;

(5) Ensure that all breaches of applicable Federal privacy law that appear to constitute a criminal violation of law, be referred for investigation to the Office of the Inspector General; and

(6) Ensure that noncompliance with these policies by VA personnel and other authorized individuals are addressed and remedied promptly.

4. REFERENCES

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

b. Government Paperwork Elimination Act of 1988, Pub. L. 105-277.

c. Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102.

d. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.

e. OMB Memo 99-18, Privacy Policies on Federal Web Sites, June 2, 1999, and attachment, Guidance and Model Language for Federal Web Site Privacy Policies.

f. OMB Memo 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Sept. 26, 2003.

g. Paperwork Reduction Act of 1995, Pub. L. 104-13.

h. Privacy Act of 1974, 5 USC 552a, Pub. L. 93-579.

i. Privacy Policies and Data Collection on Federal Web Sites, OMB Memo 00-13, June 22, 2000.

j. VA Handbook 6000, VA IRM Framework, September 17, 1997

k. VA Handbook 6102, Internet/Intranet Services, March 15, 2001.

l. VA Directive 6300, Records Information Management, January 12, 1998.

m. VA Handbook 6300.5, Procedures for Establishing & Managing Privacy Act Systems of Records, Jan. 12 1998.

n. VA Handbook 6300.5/1, Procedures for Establishing & Managing Privacy Act Systems of Records, October 5, 2000.

o. VA Directive 6310, Forms, Collections of Information, and Records Management, Dec. 18, 2001.

p. VA Handbook 6310.2, Collections of Information Procedures, Dec. 18, 2001.

q. VA Directive 6502, Privacy Program, June 30, 2003.

5. DEFINITIONS

a. **Cookies**. A cookie file is a file that resides on the client machine. It contains data passed from Web sites, so that Web sites can communicate with this file when the same client returns. The Web site only has access to the part of the cookie file that represents the interaction with that particular Web site. One common purpose of cookies is to identify Web site visitors and possibly prepare customized Web pages for them. *Persistent cookies* are stored for a length of time that is set by the Web server when it passes the cookie to the visitor's Web browser. These cookies are used to store information about the visitor between visits to a site. *Session cookies*, in contrast, are used to store information only within a single visit. These cookies are cached (stored) only while a user is visiting the Web server issuing the cookie and are deleted from the cache when the user closes the session.

b. **Machine-readable format.** The formatting of Web page Privacy Policy statements so they can be read by Web browsers or other applications designed to interpret machine-readable policy statements. Such technologies may then alert users automatically about whether site privacy practices match their personal privacy preferences.

c. **Personally Identifiable Information.** Any information about an individual that identifies that individual.

d. **Privacy Act Statements.** A set of disclosures mandated by the Privacy Act which must be made when collecting information from individuals subject to that Act.

e. **Web page** and **Web site**. A Web page is a document created with hypertext markup language (HTML) that may be part of a group of hypertext documents or resources available on the World Wide Web. Collectively, a set of these documents and resources may form a Web site. Every Web page is identified by a unique universal resource locator (URL).