Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6507
Transmittal Sheet
November 20, 2008

REDUCING THE USE OF SOCIAL SECURITY NUMBERS

I. REASON FOR ISSUE: This Directive issues policy requirements for the Department of Veterans Affairs (VA) to reduce and, where possible, eliminate the collection and use of the Social Security Number (SSN) as a primary identifier for uniquely identifying individuals in VA operations, programs and services.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: The Office of Management and Budget (OMB) issued Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, directing all Federal agencies to review and minimize their use of SSNs. The President's Task Force on Identity Theft, in a report released April, 23 2007, and entitled "Combating Identity Theft: A Strategic Plan", recommends the reduction of the use of SSNs by Federal agencies. This policy directs the Administrations and Staff Offices to develop and implement plans to reduce or eliminate the collection and use of SSNs except where a compelling business need is shown or the collection and use is authorized by law or deemed necessary to the mission of the Department, as prescribed by the Secretary.

Note: In many instances, use of the SSN will be necessary in order to maintain business continuity until such time as the VA SSN Review Board established by this Directive can evaluate and make determinations on current uses.

3. RESPONSIBLE OFFICE: Associate Deputy Assistant Secretary (ADAS), Office of Privacy and Records Management, Office of Information Protection and Risk Management, Office of the Assistant Secretary for Information and Technology (005).

4. RELATED HANDBOOK: None.

5. RESCISSION: None.

CERTIFIED BY:

/s/
Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Robert T. Howard
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

REDUCING THE USE OF SOCIAL SECURITY NUMBERS

1. PURPOSE

a. To ensure that the Department of Veterans Affairs (VA) is providing care and services to each veteran according to his or her needs, it is critical that VA be able to distinguish each individual in a unique manner. Within government, social security numbers (SSNs) are expressly authorized by statute for use as personal identifiers for numerous purposes including employment, taxation, receipt of veterans' benefits, employment verification, and law enforcement. In the private sector, the SSN is used throughout various industries, including the insurance and financial industries, as a unique personal identifier.

b. The increased availability and aggregation of personal information, including SSNs, coupled with the proliferation of information available in electronic databases and through the Internet and Intranets, has exposed SSNs to potential misuse and to possible identity theft. Thus, VA, in conjunction with all Federal agencies, must take steps to reduce and, where possible, eliminate the use of the SSN for uniquely identifying individuals in VA operations, programs and services.

c. The Office of Management and Budget (OMB) Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, among other things, requires that VA establish short and long term plans to "eliminate the unnecessary collection and use of SSNs."

d. VA is working to develop a unique identification number for use across VA information systems. However, this is not expected to be available VA-wide in the near term. In addition, while the Health Insurance Portability and Accountability Act (HIPAA) standard patient identifier provision would help VA to reduce its dependence on the SSN, there has been little progress in that direction. Until alternatives to the SSN have been identified, VA offices must develop plans to eliminate all unnecessary collection and use of the SSN and implement appropriate security controls to protect the SSN when required for use in VA business processes.

2. POLICY

a. VA must develop and implement plans to eliminate the collection and use of the SSN as a primary identifier except where the collection or use of the SSN is authorized by law or addresses a compelling business need under the mission of the Department, as prescribed by the Secretary.

b. Acceptable interim techniques for accomplishing the minimization of risk regarding the use of SSNs shall include masking, scrambling, or modification of the SSN. While embedding or truncating the SSN may be considered acceptable short-term remedies, they are not acceptable long-term fixes. Although these methods assist in minimizing risk of identity theft, they should not be considered techniques for reducing SSN use.

(1) The SSN shall not appear in any form (i.e., in its entirety, or in part) on documents to be used as identification except where a compelling business need is shown or the collection and use is authorized by law or deemed necessary to the mission of the Department.

(2) Unless required by law, deemed necessary to the mission of the Department, or where a compelling business need is shown, the full SSN may not be placed in magnetic strips, used in bar codes, or transmitted or stored in electronic form unless the data is encrypted.

c. VA will participate in government-wide efforts to explore alternatives to Department use of SSNs as a personal identifier for both Federal employees and in veterans' programs.

d. OMB guidance will direct VA's efforts in this area, as well as, the efforts of all other Federal agencies.

e. VA will implement a Unique Employee Identifier (UEID) as provided by the Office of Personnel Management (OPM) for all Federal agencies.

f. VA will implement, where feasible, the recommendations of the President's Task Force on Identity Theft and the Interagency Best Practices Collaborative that was assembled to establish best practices for the elimination of the unnecessary collection and use of SSNs throughout government.

g. VA will assemble a board to review and evaluate all current and proposed uses of the SSN. The board will be comprised of representatives from each Administration and all key Staff Offices. This board will determine whether said uses are authorized by law, required by law, fulfill a compelling business need, or none of the above. Information Owners and Information System Owners will be given reasonable opportunity to develop and implement plans to reduce SSN usage for uses the board determines are not required by law. The governance structure of this board will be addressed through a formal charter and policy, which will be issued at a later date.

3. RESPONSIBILITIES

a. **The Secretary of Veterans Affairs.** The Secretary has designated the Assistant Secretary for Information and Technology as the Department's Chief Information Officer (CIO), the senior agency official responsible for VA Information Security and Privacy Programs.

b. **The Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as VA CIO, shall:

(1) Designate the Deputy Assistant Secretary (DAS), Office of Information Protection and Risk Management, as the principal Department official responsible for ensuring department-wide compliance with this Directive;

(2) Ensure all VA-wide systems and applications currently in use, or being developed or acquired comply with the requirements of this directive;

(3) Ensure individuals are properly identified and unique identifiers can be correlated across VA Systems;

(4) Designate the Associate Deputy Assistant Secretary (ADAS), Office of Privacy and Records Management as the principal Department official responsible for overseeing the implementation of this Directive; and

(5) Submit reports to OMB on the status of VA's efforts related to the reduction or elimination of the collection and use of SSNs, as required.

c. **The Deputy Assistant Secretary (DAS), Office of Information Protection and Risk Management.** The DAS shall collaborate with the Executive Director of Oversight and Compliance; DAS, IT Enterprise Strategy, Policy, Plans and Programs; DAS, IT Resource Management; DAS, Enterprise Development; DAS Enterprise Operations and Infrastructure; and the DAS for Human Resources Management, as needed, for the implementation of this Directive.

d. **The ADAS, Office of Privacy and Records Management.** The ADAS, Office of Privacy and Records Management shall designate the Director, VA Privacy Service as the responsible officer for reviewing and providing feedback on:

(1) All plans developed by the Administrations and Staff Offices; and

(2) Quarterly implementation reports to be submitted to the CIO by the Administrations and Staff Offices.

e. **Director, VA Privacy Service.** The Director shall:

(1) Collaborate with the Administrations and Staff Offices, as needed, regarding the development of plans related to this Directive, review related plans, and provide feedback related to the adequacy and quality of the plans;

(2) Review quarterly implementation reports to be submitted to the CIO by the Administrations and Staff Offices and provide feedback, as he or she determines to be necessary; and

(3) Prepare for submission to OMB, reports on the status of efforts related to the elimination in the collection and use of SSNs, as required.

f. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials shall:

(1) Conduct an assessment of SSN collection and use throughout their areas of responsibility in order to determine the actions necessary to eliminate, restrict or conceal on forms, in business processes, and systems including, but not limited to:

(a) Conducting an inventory of all forms (paper and electronic) that collect SSNs, and evaluate whether the use of SSNs on these forms is essential to their business purpose;

(b) Analyzing all software and systems being used, acquired or developed to ensure that they comply with this Directive and, unless a compelling business need is shown or the collection and use is authorized by law or deemed necessary to the mission of the Department, does not display the SSN automatically;

(c) Reviewing all Privacy Act Systems of Record Notices (SORNs) to determine if SSNs collected and maintained as part of the system of records have appropriate SORNs; and amend SORNs as appropriate, and

(d) Evaluating whether the collection, use and maintenance of SSNs are essential to the business purpose for the system of records.

(2) Develop and implement Administration and Staff Office plans, in accordance with Appendix A, to eliminate the collection and use of SSNs where the collection or use of SSNs is not required by law, deemed necessary to the mission of the Department as set forth by the Secretary, or where a compelling business need is shown;

(3) Submit their plans to the ADAS, Office of Privacy and Records Management for review;

(4) Create and deliver quarterly implementation reports to the ADAS, Office of Privacy and Records Management, who will then submit them to the CIO; and

(5) Collaborate with other Under Secretaries, Assistant Secretaries, Other Key Officials and business associates to:

(a) Assess the impact of SSN collection and usage upon the operations of other VA entities;

(b) Identify which entities they must rely upon to reduce SSN usage; and

(c) Develop and implement action plans and create VA unique identifiers for all individuals for use as an alternative to the SSN where a compelling business need is shown, or use of the SSN is not required by law or deemed necessary to the mission of the Department as set forth by the Secretary.

4. REFERENCES.

a. Computer Security Act of 1987, Pub. L. 100-235, 101 Stat. 1724, as amended.

b. Fair Credit Reporting Act of 1970, Pub. L. 91-508, 15 U.S.C. 1681 et seq.

c. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, 42 USC § 201 et seq.

d. NIST Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems.

e. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

f. Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. 109-461.

g. VA Directive 6500, Information Security Program.

h. VA Directive 6502, Enterprise Privacy Program.

i. VA Directive 6600, Responsibility Of Employees And Others supporting VA In Protecting Personally Identifiable Information (PII).

j. VA Handbook 6300.4, Procedures for Processing Request for Records Subject to the Privacy Act.

k. VA Handbook 6310.2, Forms, Collections of Information Procedures.

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

m. 38 U.S.C 5701, Confidential Nature of Claims, 38 CFR 1.500-527.

n. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records, 37 CFR 17.500-511.

o. 38 U.S.C. 7332, Confidentiality of Certain Medical Records, 38 CFR 1.460-496.

5. DEFINITIONS

a. **Business Associate**: For the purposes of this Directive, a business associate is defined as an entity, including an individual, company, or organization that, on behalf of VHA, performs or assists in the performance of functions or activities involving the use or disclosure of Protected Health Information (PHI), or that provides certain services involving the disclosure of PHI by VHA.

b. **Compelling Business Need**: A business requirement so great as to persuade by the forcefulness of an argument in its favor.

c. **Hard Copy Media**: Physical representations of information. Paper printouts, printer, and facsimile ribbons, drums, and platens are all examples of hard copy media. These types of media are often the most uncontrolled. Information tossed into the recycle bins and trash containers exposes VA to a significant vulnerability to "dumpster divers", and overcurious employees, risking accidental disclosures.

d. **Individual**: For the purposes of this Directive, the term individual includes employees of VA (including volunteers and contractors), beneficiaries and their dependents or survivors, and others with whom VA has a business relationship and collects or stores social security numbers.

e. **Information Owner**: As defined by VA Handbook 6500, an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

f. **Information System Owner**: As defined by VA Handbook 6500, an official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

g. **Personally-Identifiable Information (PII)**: For purposes of this Privacy Service Directive, PII shall be a subcategory of VA Sensitive Information/Data as defined by VA Handbook 6500. PII is any information about an individual that can reasonably be used to identify that individual that is maintained by VA, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, etc., including any other personal information which is linked or linkable to an individual.

h. **Protected Health Information (PHI)**: For purposes of this Privacy Service Directive, PHI shall be considered a subcategory of PII. This term applies only to Individually Identifiable Health Information that is under the control of VHA, as VA's only Covered Entity under HIPAA. PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium, and relates to (i) the past, present, or future physical or mental health, or condition of an individual; (ii) provision of health care to an individual; or (iii) past, present, or future payment for the provision of health care to an individual, and that identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. *Note: PHI excludes employment records held by a covered entity in its role as an employer.*

i. **Strong Authentication**: A layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information. *(See: Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary (June 2006)).*

j. **Use**: The act or practice of employing something in order to carry out a specific purpose or action.

.

ACTION PLANS

Each Administration and Staff Office is responsible for developing and submitting a plan to eliminate the unnecessary collection and use of social security numbers (SSNs). The plans must be submitted to the ADAS for Privacy and Records Management, who will review and submit them to the VA CIO. Updates to these plans must be submitted quarterly, to the ADAS, Privacy and Records Management, who will submit them to the Chief Information Officer (CIO). These plans shall include, but are not limited to:

1. Replacing SSNs with OneVA unique identifiers on all communications and mailings unless a compelling business need is demonstrated for their retention;

2. Conducting a review of the collection and use of SSNs in order to determine the circumstances under which their use as a primary identifier may be eliminated, restricted, or concealed in agency business processes, systems, and forms (paper or electronic);

3. Removing, or suppressing SSNs in databases that are shared or mined unless required by law, deemed necessary to the mission of the Department, or a compelling business need is shown;

4. Developing plans to convert hard copy media displaying Personally Identifiable Information (PII) to electronic form;

5. Removing SSNs from all physical security/identity verification materials (e.g., identity cards and forms) unless required by law, deemed necessary to the mission of the Department, or a compelling business need is shown;

6. Ensuring that:

(a) All databases and applications that support VA-approved encryption solutions store SSNs in accordance with VA policy;

(b) Servers, tapes, disks, back-ups, and other electronic storage devices containing SSNs are housed in secure physical locations in accordance with VA policy;

(c) Only VA-approved portable electronic storage media is used to house and transport SSNs in encrypted format;

(d) Desktops, laptops, and other electronic storage devices, including portable devices containing SSNs are sanitized and disposed of in accordance with VA policy; and

(e) Paper documents displaying SSNs are maintained and disposed of, in accordance with VA policy; and maintained of in a manner that limits access only to authorized persons throughout the information lifecycle;

7. Developing processes to ensure that SSNs are not collected, used, or disseminated unless authorized by law, deemed necessary to the mission of the Department, or a compelling business need is shown, and ensuring that these processes are utilized throughout the system development lifecycle;

8. Inventorying all forms that require SSNs, and evaluating use of SSNs on these forms to ensure use is essential to their business purpose, and collaborating with internal stakeholders and external business associates as necessary to ensure changes that impact processes are evaluated and issues resolved to ensure continuity of operations;

9. All software being used, acquired or developed for VA business operations is evaluated to ensure compliance with this Directive and, unless required by law, deemed necessary to the mission of the Department, or a compelling business need is shown, prohibits automatic display of the SSN;

10. VA-approved encryption solutions are employed to protect SSNs that are transmitted via email;

11. Adopting use of OneVA unique identifiers to replace use of the SSN, and devising methods for converting and correlating SSNs to utilize the alternative unique identifier;

12. Employing strong authentication and access controls for access to VA systems and records containing PII;

13. Controlling access to records that contain SSNs, by assigning access based on need-to-know and least privilege principles, and utilizing audit trails/records to verify access;

14. All contractors and business associates adhere to the requirements set forth in this Directive; and

15. Conducting periodic audits of contracts dealing with the collection and use of the SSN for compliance with this Directive.