The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

June 4, 2007

PRIVACY POLICY GUIDANCE MEMORANDUM

Memorandum Number: 2007-02

MEMORANDUM FOR: DHS Directorate and Component Leadership

FROM: Hugo Teufel III
Chief Privacy Officer

SUBJECT: Use of Social Security Numbers at the Department of Homeland Security

I. PURPOSE

The Social Security number (SSN) is a key piece of personally identifiable information and has come to be used for numerous non-Social Security and non-legally required purposes. The widespread use of SSNs beyond their intended purpose raises privacy concerns and enables the growing problem of identity theft. In the ongoing effort to minimize the use of the Social Security number, the Privacy Office is issuing this guidance memorandum on collection, use, maintenance, and dissemination of SSNs.

DHS programs shall collect, use, maintain, and disseminate SSNs only when required by statute or regulation or when pursuant to a specific authorized purpose as outlined below. Absent these requirements, DHS programs shall not collect or use an SSN as a unique identifier; rather, programs shall create their own unique identifiers to identify or link information concerning an individual.

II. BACKGROUND

The Privacy Act of 1974 ("Privacy Act"), 5 U.S.C. § 552a, as amended, sets forth conditions on the use of an individual's SSN by any "Federal, State or local governmental agency."

There are two essential requirements to an agency's collection, use, maintenance, or dissemination of a SSN:

- No governmental agency can "deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number" except refusal to disclose after a request pursuant to requirements of federal statutes or pursuant to pre-existing federal or state statutes or regulations through which a system of records had already (before

January 1, 1975) been set up. (5 U.S.C. § 552a) (note, Section 7 Disclosure of Social Security Number)

- A government agency must accompany any solicitation of an individual's SSN with that agency's statement of whether the disclosure is mandatory or voluntary, what statutory or other authority supports the solicitation, and what uses (including internal use and external sharing) will be made of the number. (5 U.S.C. § 552a) (note, Section 7 Disclosure of Social Security Number)

All records containing SSNs are considered sensitive information.

III. GUIDANCE FOR THE USE OF SSNS BY DHS PROGRAMS.

A. New System Development

Prior to the development of a program that seeks to collect, use, maintain, and/or disseminate SSNs, the program manager will prepare a Privacy Threshold Analysis for Privacy Office review, which identifies the reason the SSN is needed. The Privacy Office, in coordination with the component Privacy Officer and the respective program, will review the program's need to collect, use, maintain, and/or disseminate the SSNs to ensure such agency action is required by statute or regulation and/or determine whether collection is authorized for this specific purpose. If the Privacy Office in coordination with the program determines that there is an adequate need and appropriate authority, the program will complete a Privacy Impact Assessment (PIA) addressing the Privacy Act requirements necessary for such collection, use, maintenance, or dissemination of the SSN, as well as the associated privacy risks.

The Privacy Office will review and approve the PIA upon proper analysis of the privacy risks. Note that as with any other personally identifiable information, an approved PIA must exist prior to any collection or use of SSNs.

B. Existing System Review

For those programs that currently collect, use, maintain, and/or disseminate SSNs, the program manager will prepare a Privacy Threshold Analysis for Privacy Office review, which identifies the reason the SSN is needed. If a PTA already exists for the system, then the program needs to update it with additional explanation regarding the need for the SSN. The Privacy Office, in coordination with the component Privacy Officer and the respective program, will review the program's need to collect, use, maintain, and/or disseminate the SSNs to ensure such agency action is required by statute or regulation and/or is pursuant to a specific authorized purpose. If the Privacy Office and the component Privacy Officer in coordination with the program determine that the collection, use, maintenance and/or dissemination of the SSN should be reduced or eliminated, the program will provide a Plan of Action and Milestones (POA&M) to the Privacy Office for approval indicating how and when this change will be implemented.

C. Notice

Pursuant to the Privacy Act of 1974 5 U.S.C. § 552a(e)(3), any request by a program to collect an SSN from an individual shall be supported by a Privacy Act statement directly to the individual stating (a) whether the disclosure is mandatory or voluntary, (b) the statutory or other authority supporting the disclosure, and (c) the reason for the disclosure. Any such notice will contain language previously approved by the Privacy Office and the Office of the General Counsel.

D. Collection/Use

SSNs may not be collected either directly or indirectly without identifying the connection between the SSN and a legal requirement or specific authorized purpose. Unless statutorily required or otherwise specifically authorized to use SSNs as unique system identifiers, programs shall create internal unique system identifiers to identify or link information about an individual within the information system.

For existing programs, the review in Section B above will occur.

E. Security

Sufficient security controls must be implemented in order to mitigate the risk of inappropriate or unauthorized disclosure of data containing SSN. Any access to SSNs shall be restricted with an appropriate application of security controls. Any program collecting, using, maintaining, and/or disseminating SSNs must maintain audit logs tracking the access to the SSNs, and the program must perform periodic reviews of these audit logs. In many cases, the existing logging process will cover this requirement.

Additionally, for the purposes of information security, any system involving SSNs shall be treated as having at least a moderate potential impact on an individual regarding the loss of confidentiality.[1] Any system deployed for a program involving SSNs must have security measures commensurate with this security categorization, such as automatic removal of user access for any user after the particular user account is unused for a period of time determined appropriate for that system. This policy requirement shall apply whether the data resides on a system, is transmitted over a network, or is contained on physical digital or paper media.

Encryption, the application of which is encouraged, will minimize the risk of unauthorized disclosure. Other security controls, such as password protection may also mitigate the risk associated with authorized disclosure. The appropriate controls will be determined by the program in coordination with the Privacy Office, Chief Information Officer, the component Privacy Officer, and the Information System Security Manager (ISSM).

---

[1] Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004).

Social Security Numbers = {(confidentiality, MODERATE)}

Personnel who access or disseminate SSNs without proper authorization may be subject to disciplinary action, including possible dismissal, as well as any penalties authorized by law.

F. Retention

In accordance with the Federal Records Act of 1950, as amended, any other applicable laws, regulations and policies, and the applicable record retention schedule, the program must destroy or dispose of the paper documents and electronic media containing SSNs using a method designed to prevent or significantly inhibit their recovery or use. SSNs shall only be retained in official agency record files. SSNs shall never be retained by an employee in a non-agency record or file.