Department of Homeland Security
DHS Directives System
Instruction Number: 047-01-010
Revision Number: 00
Issue Date: June 18, 2019

SOCIAL SECURITY NUMBER COLLECTION AND USE REDUCTION

I. Purpose

With this Instruction, the Department of Homeland Security (DHS) Chief Privacy Officer:

A. Requires the elimination of the unnecessary collection, use, maintenance, and dissemination of the Social Security number (SSN) by DHS programs, systems, and forms; or

B. Requires the use of a unique alternative identifier to the SSN; or

C. Requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN; and

D. Implements the DHS Directive 047-01, "Privacy Policy and Compliance."

II. Scope

A. This Instruction applies throughout DHS.

B. The Privacy Policy Guidance Memorandum 2007-02/DHS Policy Directive 140-11, "Regarding the Use of Social Security Numbers at DHS," is hereby cancelled.

III. Authorities

A. Section 222 of the Homeland Security Act of 2002, as amended (6 U.S.C. § 142)

B. The Privacy Act of 1974 ("Privacy Act"), 5 United States Code (U.S.C.) § 552a, as amended

C. Public Law No. 115-59, "Social Security Number Fraud Prevention Act of 2017," 42 U.S.C. § 405 note

D. Title 44, U.S.C., Chapter 35, Subchapter III, “Information Security” [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]

IV. References

A. OMB Circular A-130: Managing Information as a Strategic Resource (July 2016)

B. DHS Directive 047-01, “Privacy Policy and Compliance”

C. DHS Directive 140-01, “Information Technology Security Program”

D. DHS Privacy Policy Directive 140-06, “The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security”

E. DHS Privacy Policy Directive 140-09, “DHS Policy Regarding Privacy Impact Assessments”

F. DHS Instruction 047-01-006, “Privacy Incident Responsibilities and Breach Response Team”

G. DHS Instruction 047-01-007, “Handbook for Safeguarding Sensitive Personally Identifiable Information”

H. DHS Sensitive Systems Policy Directive 4300A

I. DHS 4300A, “Sensitive Systems Handbook”

J. DHS Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 2017)

V. Definitions

A. ***Privacy Compliance Documentation***: Any document required by statute or by the Chief Privacy Officer pursuant to DHS Directives and Instructions that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Impact Assessments (PIA), System of Records Notices (SORN), Privacy Threshold Analyses (PTA-see next page), Notices of Proposed Rulemaking for Exemption to Privacy Act System of Records (NPRM), and Final Rules.

B. ***Privacy-Enhancing SSN Alternatives***: Is an alternative to eliminating the SSN when there are technological, legal, or regulatory limitations. Examples of privacy-enhancing alternatives include masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.

C. ***Privacy Threshold Analysis (PTA)***: Serves as the official determination by the DHS Privacy Office as to whether a Department program or system has privacy implications, and if additional privacy compliance documentation is required, such as a Privacy Impact Assessment (PIA) or System of Records Notice (SORN). The PTA is built into departmental processes, including for forms, technology investments, and security. PTAs expire and must be reviewed and re-adjudicated at least every three years. PTAs must also be updated whenever there is a change to a program, system, or form.

D. ***Program Manager***: The DHS employee who is responsible for the planning and operation of a DHS program/system.

E. ***Unique Alternative Identifiers***: A unique set of characters and/or numbers, used in place of an SSN, generated and assigned to an individual that uniquely identifies each individual. Such an identifier is not created from or associated with any other information about the individual. Unless stated within the program and agency-specific purpose described in the PTA, the identity of an individual cannot be directly or indirectly inferred, nor linkable to an individual from the alternative identifier information, without the use of an algorithm or appropriate encryption.

VI. Responsibilities

A. ***Chief Privacy Officer***: In addition to the responsibilities outlined in DHS Directive 047-01:

1. Coordinates with the Component Privacy Officer or Privacy Points of Contact (PPOCs) to ensure that the Component use of SSNs is in compliance with this policy; and

2. Reviews and approves privacy compliance documentation for the collection, maintenance, and use of SSNs.

B. ***Component Privacy Officer***:

1. Maintains an accurate account of all Component use of SSNs, and ensures that programs and systems implement this Instruction with respect to the use of SSNs; and

2. Coordinates with Program Managers to create a method of generating an alternative identifier to the SSN, or implementing privacy-enhancing SSN alternatives.

C. ***Privacy Points of Contact (PPOCs)***: Assume the duties of Component Privacy Officers, as defined above, in Components that do not have Privacy Officers.

1. Coordinates with the Chief Privacy Officer, or designee, to ensure that programs and systems implement this Instruction with respect to the use of SSNs; and

2. Coordinates with the Chief Privacy Officer, or designee, and Program Managers to create a method of generating an alternative identifier to the SSN, or implementing privacy-enhancing SSN alternatives.

D. ***Chief Information Officer (CIO)***: Evaluates the implementation and effectiveness of security safeguards when assessing the likelihood of access and use of SSNs potentially compromised by a privacy incident, in accordance with DHS policy, including DHS Instruction 047-01-006.

E. ***Chief Information Security Officer (CISO)***: Provides security oversight and information assurance for all DHS information systems, including assessing the risk and magnitude of harm to such systems resulting from a privacy incident, in accordance with DHS policy, including DHS Instruction 047-01-006.

F. ***Component IT Security Entity***: Evaluates the implementation and effectiveness of implemented security safeguards, such as password-protection or encryption, and mitigates the risk of a privacy incident. The Component IT Security Entity can include the Component Information Systems Security Manager (ISSM), the Component Security Incident Response Center (CSIRC), or Component Security Operations Center (SOC).

G. ***Program Manager***:

1. Coordinates with the Component Privacy Officer or PPOC to create a method of generating unique alternative identifiers or implementing privacy-enhancing SSN alternatives;

2. Coordinates with the Component Privacy Officer or PPOC to prepare drafts of all privacy compliance documentation as required when proposing, developing, implementing, or changing any use of SSNs in compliance with DHS policy and this instruction;

3. Monitors the design, deployment, operation, and retirement of programs involving collection or use of SSNs to ensure that the collection or use of the SSN is limited to what is described in the privacy compliance documentation;

4. Coordinates with the Component Privacy Officer or PPOC and DHS Privacy Office to establish administrative, technical, and physical controls for storing and safeguarding the SSN and any alternative identifier consistent with DHS privacy, security, and records management requirements to ensure protection from unauthorized access, disclosure, or destruction; and

5. Maintains and monitors audit logs that track access to SSNs and alternative identifiers for periodic review by the DHS Privacy Office and Component Privacy Office.

VII. Content and Procedures

A. ***New Program/System or Form Development***: For any proposed program, system, or DHS-specific form that plans to collect, use, maintain, and/or disseminate SSNs, the DHS Privacy Office requires program managers, even if their program, system, or form is properly authorized to collect SSNs, to create and use a unique alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, the DHS Privacy Office requires privacy-enhancing SSN alternatives.

1. This requirement is documented in the Privacy Threshold Analysis (PTA) when seeking approval for the new program, system, or form.

2. Approved DHS-specific forms containing SSNs that will be mailed through the U.S. Postal Service (USPS) must have the SSN masked or redacted, or be sent via a secure method.

B. ***Existing Program/System or Form Review***: During the PTA review process, program managers are required to create and use a unique alternative identifier for any existing program, system, or DHS-specific form that is currently authorized to collect, use, maintain, and/or disseminate SSNs. If there are technological, legal, or regulatory limitations to eliminating the SSN, the DHS Privacy Office requires privacy-enhancing SSN alternatives. DHS-specific forms containing SSNs that will be mailed through the USPS must have the SSN masked or redacted, or be sent via a secure method.

C. ***Notice***: A DHS program/system that requests an individual to provide an SSN directly from the individual must provide a Privacy Act Statement, required by the Privacy Act, 5 U.S.C. 552a(e)(3) and 552a(note)(Disclosure of Social Security Number), or a Privacy Notice, as required by DHS policy. The Statement or Notice must state (a) whether the disclosure to DHS is mandatory or voluntary, (b) the statutory or other authority such number is solicited to support the disclosure to DHS, (c) the principal purpose or purposes for which the information is intended to be used by DHS, (D) the uses by DHS that may be made of the information, including disclosures made outside of DHS, and (E) the effects on the individual, if any, of not providing the SSN to DHS. Any such notice will contain language previously approved by the DHS Privacy Office or Component Privacy Officer, if authorized by the Chief Privacy Officer, and the Office of the General Counsel or Component counsel.

D. ***Security***:

1. Sufficient security controls as required by law (e.g., Privacy Act of 1974, 5 U.S.C. 552a(e)(10)) and policy must be implemented in order to mitigate the risk of inappropriate or unauthorized disclosure of data containing SSN or alternative identifier. Any access to SSNs or alternative identifiers shall be restricted with an appropriate application of security controls. Any program/system collecting, using, maintaining, and/or disseminating SSNs or alternative identifiers must maintain audit logs that track access to, and disclosure of, the SSNs or alternative identifiers. The Component Privacy Officer or PPOC completes periodic reviews of these audit logs or as requested by the Chief Privacy Officer.

2. Any system involving SSNs shall be treated as having at least a moderate potential impact on an individual regarding the loss of confidentiality. 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 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.

3. Apply encryption technologies when feasible to minimize the risk of unauthorized disclosure. Other security controls, such as password protection, may also mitigate the risk associated with unauthorized disclosure. The appropriate controls will be determined by the program/system in coordination with the DHS Privacy Office, Component Privacy Officer or PPOC, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Records Officer (CRO), Component Privacy Officer, and a representative from Component IT Security Entity.

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

E. ***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/system must destroy or dispose of paper documents and electronic media containing SSNs or alternative identifiers using a method designed to prevent or significantly inhibit their recovery or use. SSNs and alternative identifiers shall only be retained in official agency record files.

VIII. Questions

Address any questions or concerns regarding this Instruction to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.

6/18/2019

Jonathan R. Cantor
Chief Privacy Officer, Acting

Date