**Department of Homeland Security**
**DHS Directives System**
**Directive Number: 047-01**
**Revision Number: 00**
**Issue Date: 7/7/2011**

# PRIVACY POLICY AND COMPLIANCE

## I. Purpose

This Directive establishes privacy policy for the Department of Homeland Security (DHS or Department).

## II. Scope

This Directive applies throughout DHS regarding the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information (PII) and regarding any other activity that impacts the privacy of individuals as determined by the Chief Privacy Officer.

## III. Authorities

A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note]

B. Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]

C. Title 6 U.S.C. Section 142, "Privacy officer"

D. Title 44, U.S.C., Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)]

E. Delegation 2050.1, "Delegation to the Chief Privacy Officer"

## IV. Responsibilities

A. The ***Chief Privacy Officer*** is responsible for:

1. Establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy;

2. Ensuring, in coordination with Component heads and Component

Privacy Officers and Privacy Points of Contact (PPOC), that the Department follows DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies in collecting, using, maintaining, disclosing, deleting, and/or destroying PII, and in implementing any other activity that impacts the privacy of individuals;

3. Ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII;

4. Evaluating Department regulations, rulemakings, technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts and advising DHS leadership and Components on implementing corresponding privacy protections;

5. Reviewing and approving all Department Privacy Compliance Documentation;

6. Implementing DHS Privacy Act regulations in accordance with Department procedures and amending those regulations as necessary to reflect changes in relevant law and Department policy;

7. Ensuring that the Department meets all reporting requirements mandated by Congress or the Office of Management and Budget (OMB) regarding DHS activities that involve PII or otherwise impact privacy;

8. Coordinating with the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) to provide guidance regarding information technology and technology-related programs and to develop and implement policies and procedures to safeguard PII used or maintained by the Department in accordance with federal law and policy;

9. Ensuring that all DHS interagency and international information sharing agreements comply with DHS Privacy Compliance Documentation requirements and DHS privacy policy;

10. Providing educational outreach on Privacy Compliance Documentation and on emerging privacy issues and policies to the Department's international partners;

11. Counseling the Department and other federal agencies on existing and emerging changes in global privacy practices and policies;

12. Investigating and mitigating, where appropriate, privacy incidents or matters relating to possible violations of privacy arising from the

administration of any Department program or operation, where the Inspector General declines to investigate following referral of a privacy incident or matter by the Chief Privacy Officer;

13. Processing privacy complaints from organizations and individuals regarding Department activities and ensuring that redress is provided, where appropriate;

14. Developing and overseeing mandatory and supplementary privacy training for DHS employees, including training on privacy compliance procedures, privacy incident handling, and privacy complaint handling, and conducting DHS-wide privacy training programs;

15. Coordinating with the Office for Civil Rights and Civil Liberties on issues of concern to both offices arising from Department activities;

16. Serving as the Department's Senior Agency Official for Privacy (SAOP) for OMB purposes;

17. Serving as the Department's official point of contact on all matters related to privacy in the Federal Government;

18. Serving as an *ex officio* member of the Information Sharing Governance Board (ISGB) in accordance with the ISGB Charter, and participating in and providing guidance to any other DHS entity or initiative related to information sharing; and

19. Serving as the DHS Information Sharing Environment Privacy Official.

B. ***Component Heads*** are responsible for:

1. Implementing DHS privacy policy and procedures established by the Chief Privacy Officer;

2. Ensuring completion of their respective Components' Privacy Compliance Documentation in a timely manner;

3. Assisting the Chief Privacy Officer in investigating and reviewing Component activities to ensure that privacy protections are fully integrated into Component operations and that privacy incidents and privacy complaints are addressed and redress provided, where appropriate;

4. Ensuring that their respective Components provide the Chief Privacy Officer all information necessary to meet the Department's reporting requirements regarding privacy-related DHS activities;

5. Providing financial resources and other support for their respective Component Privacy Officers or PPOCs, to ensure effective implementation of all aspects of DHS privacy policy; and

6. Ensuring that Component contracts for activities that involve PII or otherwise impact the privacy of individuals include appropriate language requiring that Department contractors follow DHS privacy policy and this Directive.

# V. Policy and Requirements

1. The Department adopts the Fair Information Practice Principles (FIPPs) set forth in Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 29, 2008) (attached to this Directive) as privacy policy for DHS.

2. The Chief Privacy Officer determines privacy policy and standards for the Department consistent with the FIPPs; oversees compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies; provides privacy guidance and training to DHS personnel regarding the FIPPs; and provides support on privacy-related matters to senior Department leadership and to the Components. Component heads work with the Chief Privacy Officer to ensure that Department activities follow DHS privacy policy and standards, thereby enhancing the overall consistency of privacy protections across DHS.

# VI. Cancellation

DHS Directive 0470.2, "Privacy Act Compliance," is hereby canceled.

# VII. Questions

Address any questions or concerns regarding this Directive to the DHS Privacy Office.

Rafael Borras
Under Secretary for Management

7/7/11
Date

**Attachment**
**Directive 047-01**

***The Fair Information Practice Principles Framework for Privacy Policy at the Department of Homeland Security***

**Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII.

**Individual Participation:** DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

**Purpose Specification:** DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

**Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

**Use Limitation:** DHS should use PII solely for the purpose(s) specified in the system of records notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

**Data Quality and Integrity:** DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

**Security:** DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

**Accountability and Auditing:** DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.