

PRIVACY POLICY FOR RESEARCH PROGRAMS AND PROJECTS

I. Purpose

This Directive establishes the Department of Homeland Security (DHS or Department) privacy policy for DHS privacy-sensitive research programs and projects.

II. Scope

This Directive applies to all privacy-sensitive research programs and research projects conducted throughout DHS, except with regard to privacy-sensitive research conducted by the Office of Inspector General as part of its investigation and audit functions.

III. Authorities

- A. Public Law 107-347, Section 208, "The E-Government Act of 2002," as amended
- 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 42, U.S.C., Section 2000ee-1, "Privacy and civil liberties officers"
- E. Title 44, U.S.C., Chapter 35, Subchapter III. "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)]
- F. Delegation 13001, "Delegation to the Chief Privacy Officer"

IV. Responsibilities

- A. The **Chief Privacy Officer** is responsible for ensuring that the Department's use of technology sustains privacy protections relating to the collection, disclosure, retention, and destruction of Personally Identifiable Information (PII); determining whether a particular research program or project is

privacy-sensitive; reviewing privacy guidance developed by Component Privacy Officers to ensure consistency in privacy policy across the Department; assisting the Secretary and Component heads in addressing potential privacy impacts when such officials are proposing, developing, or implementing research programs or projects, including pilot programs; ensuring that research technologies, programs, and projects include privacy protections to address identified or potential privacy impacts; reviewing and approving all privacy compliance documentation including Privacy Threshold Analyses, Privacy Impact Assessments, and System of Records Notices; educating and training DHS personnel on the handling of PII, privacy compliance requirements, and other privacy-related matters; and working within the Department to ensure that adequate procedures are in place to receive, investigate, respond to, and, where appropriate, provide redress for complaints from individuals who allege privacy violations.

B. **Component Heads** are responsible for implementing DHS privacy policies and procedures as determined by the Chief Privacy Officer; consulting with the Chief Privacy Officer prior to proposing or developing privacy-sensitive research programs or projects, including pilot projects, to ensure appropriate consideration of the privacy impact of such activities; ensuring that privacy protections are integrated into Component research operations; appointing a full-time, senior level, Component Privacy Officer as required by the Secretary (or, where not required by the Secretary, a Privacy Officer or Privacy Point of Contact) with day-to-day responsibility for implementing DHS privacy policy and procedures for the Component; ensuring that DHS contracts for activities involving PII include appropriate language requiring that Department contractors follow this Directive; and, in the case of privacy-sensitive research programs or projects conducted with other Federal agencies, ensuring that those agencies protect PII consistent with this Directive.

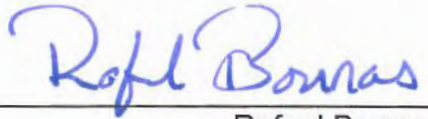
V. Policy and Requirements

The Department adopts the Principles for Implementing Privacy Protections in DHS Research Projects first enunciated in the 2008 Report to Congress on Data Mining: Technology and Policy (December, 2008) (attached to this Directive) as privacy policy for all DHS privacy-sensitive research.

The Chief Privacy Officer determines privacy policy and standards for DHS privacy-sensitive research programs and projects consistent with the Principles for Implementing Privacy Protections in DHS Research Projects; provides privacy guidance and training to DHS personnel involved in privacy-sensitive research; and provides support on privacy-related matters to DHS Components' research efforts. Component heads work with the Chief Privacy Officer to ensure that privacy-sensitive research programs and projects follow DHS privacy policy and standards, thereby enhancing the overall consistency of privacy protections across DHS research.

VI. Questions

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



Rafael Borrás
Under Secretary for Management



Date

**Attachment
Directive 140-06**

Principles for Implementing Privacy Protections in DHS Research Projects

Privacy Assessment Principle: An assessment of privacy impacts is integral to the development and implementation of any DHS privacy-sensitive research program or project.

- All programs and projects complete a Privacy Threshold Analysis (PTA) in accordance with a Component privacy implementation plan. DHS Privacy Office staff and the Component Privacy Officer or Privacy Point of Contract (PPOC) review each PTA to determine how best to apply these Principles to each privacy-sensitive program or project.
- The Privacy Office assists the Component Privacy Officer or PPOC, as appropriate, in identifying privacy impacts to address in a privacy-sensitive program's or project's design and implementation, to ensure that privacy-sensitive research programs or projects sustain privacy protections relating to the collection, use, disclosure, retention, and destruction of Personally Identifiable Information (PII) pursuant to 6 U.S.C. § 142(a)(1). An appropriately cleared Component or external expert participates in the privacy assessment to explain scientific aspects of a proposed privacy-sensitive research program or project where a deeper understanding is needed to make decisions regarding the use of PII.

Purpose Specification Principle: A privacy-sensitive program or project's purpose is clearly articulated and documented through an internal/external project review process.

- **Legal Authorization:** Programs and projects are structured to function consistently with all relevant legal requirements.
- **Purpose Limitation:** Programs and projects only engage in research that is within the scope of the documented purpose(s).
- **Effectiveness Reviews:** Programs and projects determined by the Chief Privacy Officer through a Privacy Threshold Analysis to be privacy-sensitive include an initial internal review by Component staff other than the program or project's proponents. The results of this review are provided to the Chief Privacy Officer before commencement of research involving PII. If the Chief Privacy Officer and the impacted Component then jointly determine that an additional, external review (by experts with appropriate security clearances) is required, that review will assess the program's or project's likely effectiveness in accomplishing the documented purpose(s) in accordance with the Component implementation plan.

Data Quality and Integrity Principle: Programs and projects endeavor to only use PII that is reasonably considered accurate and appropriate for the documented purpose(s), and to protect the integrity of the data.

- Programs and projects exercise due diligence in evaluating the accuracy and relevance of any publicly-available or commercially-available data used, to ensure the research effort's soundness and the integrity of the research results.

Data Minimization Principle: Programs and projects use the least amount of PII consistent with the documented purpose(s), and use PII minimization techniques such as synthetic data or anonymization where appropriate and practicable.

Use Limitation Principle: Programs and projects use PII consistent with all applicable System of Records Notices (SORNs), Privacy Impact Assessments (PIA), and other privacy notices and policies, regardless of the source of the data (*i.e.*, whether the data is collected directly by DHS or its contractors, or is obtained by DHS or its contractors from third-party sources).

Data Security Principle: Programs and projects take all reasonable steps necessary to maintain the security of the PII being used, and to protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

Audit Principle: Programs and projects involving PII employ automated and/or non-automated auditing procedures, as appropriate, to ensure compliance with project access and data usage rules ("rules" are specific instructions implementing an applicable project policy, notice, and/or legal requirement).

Transparency Principle: Programs and projects involving PII foster public trust by publishing PIAs and other public notices, except where the research is classified or Law Enforcement Sensitive (LES), or involves Security Sensitive Information (SSI), Protected Critical Infrastructure Information (PCII), or Chemical Security Information (CSI). PIAs are conducted for classified, LES, SSI, PCII, and CSI research projects, and when possible, a redacted version is published.

Redress Principle: Redress programs to handle inquiries and complaints regarding any research projects involving PII are developed in consultation with the Chief Privacy Officer, Component Privacy Officer or PPOC, and the DHS Screening Coordination Office as appropriate.

Training Principle: The Privacy Office, in conjunction with the Component Privacy Officer or PPOC, provides privacy training for all program or project personnel regarding DHS privacy policy and any privacy protections specific to a particular project.