

## **PRIVACY POLICY FOR RESEARCH PROGRAMS AND PROJECTS**

---

### **I. Purpose**

This Instruction implements Department of Homeland Security (DHS) Directive 140-06, "Privacy Policy for Research Programs and Projects."

### **II. Scope**

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

### **III. References**

- 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 44, U.S.C., Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)]
- E. Directive 026-04, "Protection of Human Subjects"
- F. Privacy Policy Guidance Memorandum 2008-02, "DHS Policy Regarding Privacy Impact Assessments" (December 30, 2008) (available on the DHS Privacy Office website at [http://www.dhs.gov/files/publications/gc\\_1271701587683.shtm](http://www.dhs.gov/files/publications/gc_1271701587683.shtm))
- G. Privacy Policy Guidance Memorandum 2008-01, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security"

Security” (December 29, 2008) (available on the DHS Privacy Office website at [http://www.dhs.gov/files/publications/gc\\_1271701587683.shtm](http://www.dhs.gov/files/publications/gc_1271701587683.shtm))

H. Privacy Policy Guidance Memorandum 2007-01, “Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons” (as amended on January 7, 2009) (available on the DHS Privacy Office website at [http://www.dhs.gov/files/publications/gc\\_1271701587683.shtm](http://www.dhs.gov/files/publications/gc_1271701587683.shtm))

## IV. Definitions

A. **Personally Identifiable Information (PII)** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information includes a name, social security number, date and place of birth, mother’s maiden name, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

B. **Privacy Impact Assessment (PIA)** means the DHS Privacy Office process and document used to describe what information DHS is collecting in connection with a research program or project or other program, project or system, why the information is being collected, how the information will be used and shared, how the information may be accessed, how the information will be protected from unauthorized use or disclosure, and how long it will be retained. The PIA also provides an analysis of the privacy considerations posed by a research program or project and the steps DHS has taken to mitigate any impact on privacy.

C. **Privacy-Sensitive Research** means research that uses or otherwise involves PII, as well as other research determined by the Chief Privacy Officer, through a Privacy Threshold Analysis, to impact the privacy of individuals.

D. **Privacy Threshold Analysis (PTA)** means the DHS Privacy Office process and document used to identify programs, projects, and systems that are privacy-sensitive and assess the need for further privacy compliance analysis. The program’s or project’s manager completes the PTA in consultation with the Component Privacy Officer or, where appropriate, the Privacy Point of Contact in accordance with the Component’s privacy implementation plan. The Chief Privacy Officer then reviews the PTA to determine whether the program or project is privacy sensitive and whether a new or updated PIA and/or System of

Records Notice is required.

E. **System of Records Notice (SORN)** means the official public notice of a DHS system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, and (4) the ways in which the information is generally shared by the Department. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS maintains about them. The Chief Privacy Officer issues all DHS SORNs.

## V. Responsibilities

A. **Component Privacy Officers** are responsible for managing the overall Component privacy program; ensuring that privacy protections are included in all of their respective Components' privacy-sensitive research programs and projects; ensuring that privacy-sensitive research programs and projects follow the Research Privacy Principles; and, in consultation with the relevant Program Manager, Component Head (or designee), and the Chief Privacy Officer, developing an implementation plan to integrate the Research Privacy Principles in all research programs and research projects covered by Directive 140-06.

B. **Privacy Points of Contact (PPOCs)** assume the responsibilities of Component Privacy Officers in DHS Components that do not have Privacy Officers.

C. **Program Managers** are directly responsible for planning, developing, and/or executing privacy-sensitive research programs and projects; conducting privacy-sensitive research in a manner that comports with the Privacy Research Principles; consulting with the Component Privacy Officer (or PPOC, where appropriate) and the Chief Privacy Officer to ensure that privacy protections, as determined by the Research Privacy Principles, are implemented in privacy-sensitive research programs and projects for which they are responsible; preparing a PTA and, where required either by the E-Government Act of 2002 or by the Chief Privacy Officer, a PIA for each research program or project; and ensuring that a SORN is in place, when required by the Privacy Act, for each program or project.

D. **The DHS Screening Coordination Office**, as appropriate and in conjunction with the Chief Privacy Officer and the relevant Component Privacy Officer or PPOC, is responsible for ensuring that a redress program to handle inquiries and complaints regarding any DHS privacy-sensitive research program or project is consistent with DHS redress policies and practices.

## VI. Content and Procedures

A. Component Privacy Officers, PPOCs, and Program Managers ensure that DHS privacy-sensitive research programs and projects implement the Principles for Implementing Privacy Protections in DHS Research Projects set out in the Attachment to Directive 140-06 (Research Privacy Principles).

B. Component Privacy Officers (or PPOCs, where appropriate) and Program Managers implement the Research Privacy Principles pursuant to privacy implementation plans developed in consultation with the Component head (or designee) and the Chief Privacy Officer.

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

1. All programs and projects complete a PTA in accordance with the Component privacy implementation plan. DHS Privacy Office staff and the Component Privacy Officer or PPOC review each PTA to determine how best to apply these Principles to each privacy-sensitive program or project.

2. The DHS 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 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.

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

1. ***Legal Authorization***: Programs and projects are structured to function consistently with all legal privacy requirements.

2. ***Purpose Limitation***: Programs and projects only engage in research that is within the scope of the documented purpose(s).

3. ***Effectiveness Reviews***: Programs and projects determined by the Chief Privacy Officer through a PTA to be privacy-sensitive include an

initial internal review by Component staff other than the program or project's proponents. The results of that 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.

E. **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.

F. **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.

G. **Use Limitation Principle**: Programs and projects use PII consistent with all applicable SORNs, PIAs, 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).

H. **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.

I. **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).

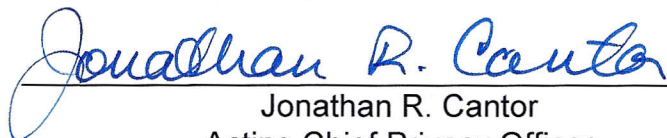
J. **Transparency Principle**: Programs and projects involving PII foster public trust by publishing PIAs and other public notices, except where the research is classified or Law Enforcement Sensitive (LES) or involves Sensitive Security Information (SSI), Protected Critical Infrastructure Information (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.

K. **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.

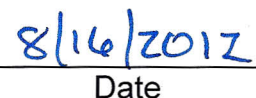
L. **Training Principle**: The Privacy Office, in conjunction with the Component Privacy Officer or PPOC, provides privacy training for all program or project personnel regarding DHS privacy policy and any privacy protections specific to a particular project.

## VII. Questions

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

  
Jonathan R. Cantor

Acting Chief Privacy Officer

  
Date