Policy Cover Sheet
For
Data Breach Policy

Policy Number: **DS-022**

Effective Date: When Signed ***Date Last Revised:*** December 11, 2006

Purpose: Provide guidelines for notification when a data breach occurs

Scope: Reported, Known, or Expected Breaches of Personally Identifiable Information (PII).

Policies and Procedures Impacted:

- ***Relationship to Mission and Privacy Principles:***

We must maintain the cooperation of respondents in order to meet our mission of being the leading source of quality data about our nation. Respondents must trust that we will keep their information confidential and take appropriate action to mitigate risks of data disclosure.

  - U. S. Census Bureau Privacy Principles:
    - Confidentiality.
    - Openness
- ***Relationship to Existing Policies, Relevant Laws and Regulation, and Procedures:***
  - The Privacy Act of 1974.
  - Office of Management and Budget (OMB) Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.
  - Identity Theft Task Force Memorandum, September 19, 2006, Identity Theft Related Data Security Breach Notification Guidance.

Responsibility for Implementation:
Chief Privacy Officer.

Committee Responsible for Ensuring the Continued Efficacy of this Policy:
The Privacy Policy and Research Committee (PPRC) is responsible for maintaining and updating this training material, based on guidance from the Data Stewardship Executive Policy (DSEP) Committee.

Contact: Gerald W. Gates ***Division:*** Privacy Office

Room Number: 8H168 ***Phone Number:*** 301-763-2515

DS-022 DATA BREACH POLICY

I. TITLE: DS0-022 Data Breach Policy

II. PURPOSE/STATEMENT OF PROBLEM

The purpose of this policy is to establish procedures for responding to a "breach of personally identifiable information (PII)"[1]. In the event of a breach of personally identifiable information (PII), this policy establishes procedures for action to be taken, by whom, and for notifying affected individuals and others who have a need to know.[2] Each incident involves unique circumstances that must be assessed in order to ensure the action and response is appropriate. This may or may not include notifying individuals and providing remedy.

III. LEGAL AUTHORITIES

- The Privacy Act of 1974. The Privacy Act of 1974[3] requires agencies to establish:
  - "…rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and the requirements of the [Act], including any other rules and procedures adopted pursuant to this [Act] and the penalties for noncompliance…,"
  - "…appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained." (5 U.S.C. § 552a(e)(9)-(10)).
- Office of Management and Budget Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments. Requires agencies to:
  - "…report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident."
- Identity Theft Task Force Memorandum, September 19, 2006, Identity Theft Related Data Security Breach Notification Guidance. Recommends that:

[1] Information covered by this policy may be in written form (on paper) or may reside electronically on traditional devices such as computer mainframes, servers, personal computers (desktop or laptops), PDAs (blackberrys) or removable media such as flash drives and memory sticks.
[2] Need to know is defined as having a work-related purpose for the information.
[3] 5 U.S.C. § 552a.

- Agencies should immediately identify a core response group that can be convened in the event of a breach.

- If an incident occurs, the core response group should engage in a risk analysis to determine whether the incident poses problems related to identity theft.

- If it is determined that an identity theft risk is present, the agency should tailor its response (which may include advice to those potentially affected, services the agency may provide to those affected, and public notice) to the nature and scope of the risk presented.

IV. SCOPE

This policy establishes guidelines for action in the case of a breach of PII. For the purposes of this policy, note the following definitions:

- **Breach** – loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an authorized purpose have access or potential access to personally identifiable information in usable form, whether physical or electronic.

- **Incident** – a violation or imminent threat of violation[4] of data protection policies, acceptable use policies, or standard security practices.

- **External notification** – The process of informing individuals about incidents such as security breaches that have caused their personal information to be acquired by unauthorized persons.

- **Personally identifiable information (PII)**[5] – any information about an individual maintained by the Census Bureau, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual regardless of the source or authority (e.g. Title 5, Title 13, Title 15, Title 26,etc.).

[4] Refers to a situation where there is a factual basis for believing that a specific incident is about to occur.
[5] OMB Memo-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments."

V. BACKGROUND

Recent Congressional and OMB action have provided initial guidance on protecting data from identity theft, which is the basis for this policy. However, the focus of this policy extends beyond identity theft because our data are at minimal risk for such criminal purposes.

A primary objective of the Census Bureau is to protect the privacy of individuals who have entrusted the Census Bureau with their personal information. The Census Bureau must strive to preserve its reputation as a data collection agency that places the highest priority on protecting the confidentiality of respondents' data and their use solely for statistical purposes. The Census Bureau cannot afford to have its mission compromised by breaches – real or perceived – in these areas.

- This policy is in direct support of Strategic Objective 4.2: Foster trust and cooperation of the public by respecting privacy and protecting the confidentiality of respondents' information.
- The Census Bureau must inform its workforce and implement procedures for the reporting and handling of potential data breaches. Appropriate responses to potential breaches demonstrate to employees and the public that we take our responsibility for the stewardship of data seriously.
- Rise in identity theft heightens public concern over any potential data loss. We must be able to respond quickly and appropriately to maintain the public's trust.
- Our privacy principle of Confidentiality is to ensure that only those that have a need to know have access to our data.
- The Privacy Act requires that we protect data, thus, we must respond appropriately to data at risk of disclosure.
- OMB requires that agencies report all breaches and provide recommendations on how to handle breaches.

VI. POLICY

The Census Bureau will identify and assess each data breach and consider providing notification, and in some cases, free credit monitoring for affected individuals based on risk scores that consider the probability that the information will be used to harm the individual.

- **Policy Requirements**

  - All potential (actual or suspected) data loss/breach incidents will be reported via the Census Bureau's Computer Incident Response Team (CIRT).
  - Incidents reported via the CIRT are reviewed weekly by the Chief Privacy Officer (CPO), Chief Information Officer (CIO), and Chief, IT Security Office. Incidents are referred to the Data Breach Team as described below. Weekly reviews that identify trends in incidents will be discussed for identifying potential actions to decrease or limit occurrences.
  - The CIRT will continue to notify the US-Cert according to requirements.

- Identified breaches are referred to the Data Breach Team for assessment. Assessments will be guided by the procedures outlined in the Data Breach Policy Implementation Guide.
- The Data Breach Team conducts a risk assessment and assigns a risk score.
- The Data Breach Team determines what action to take based on the risk score and other factors associated with the breach. Action may result in notification to individuals, providing credit monitoring services, and notifying law enforcement, if warranted.
- All data sharing arrangements will be covered by an agreement that provides for the Census Bureau to follow the guidelines of this policy in the event of a data breach. If the organization involved has a Data Breach Policy, the Census Bureau has the option to follow either policy as appropriate and in the best interest of the Census Bureau.

VII. IMPLEMENTATION

The complete implementation details can be found in the Data Breach Policy Implementation Guide.

❑ Responsibilities for Implementation

- The Privacy Office will provide privacy training and information on its Intranet site on identifying breaches and how to report incidents via the CIRT. The CPO participates in reviews of the incidents reported on the CIRT. The CPO serves as a member of the Data Breach Team.
- The CIO participates in the weekly review of incidents reported on the CIRT and serves as a member of the Data Breach.
- The Chief, IT Security Office (ITSO) provides training and information on the ITSO Intranet site on identifying breaches and how to report incidents. The ITSO manages the CIRT, participates in the weekly reviews of incidents reported on the CIRT, and serves as a member of the Data Breach Team.
- The CIRT completes the weekly CIRT report.
- The Human Resources Division (HRD) provides training on the importance of the safe handling of data during the New Employee Orientation and Time and Attendance system training.
- Employees are responsible for knowing the policies and requirements for safe data handling and proper and timely reporting of incidents to the CIRT.
- The Data Breach Team will consist of the following members: Senior Agency Official; Chief Privacy Officer; Chief Information Officer; Chief, ITSO; Associate Director for Communications; and Chief, Office of Analysis and Executive Support. Others as warranted: Chief, Office of Security; General Counsel; Inspector General; and appropriate law enforcement.

❑ Implementation Awareness Strategies

The new Privacy Awareness training module and training on the new electronic Time and Attendance system will be used to communicate to all employees how to identify and report potential breaches.

Additionally, information on how to identify and report a breach will be provided on the Census Bureau Intranet site both through the IT Security Office site and the Privacy Office site.

- **Implementation Measures**
  - Completion of weekly review of incidents reported via the CIRT by the CPO, CIO, and Chief, IT Security Office.
  - Assessment of incidents by Data Breach Team and resulting response.

VIII. REFERENCES

Federal laws define "identifying information" broadly. *See, e.g.,* The 1998 Identity Theft Assumption and Deterrence Act (Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028)) and the Fair and Accurate Credit Transactions Act (15 U.S.C. §§8 1681-1681x, as amended). This memorandum focuses on the type of identifying information generally used to commit identity theft.

IDENTITY THEFT TASK FORCE MEMORANDUM, September 19, 2006, Identity Theft Related Data Security Breach Notification Guidance.
http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf

IX. DATE POLICY BECOMES EFFECTIVE: Upon Signature

X. SIGNATURE AND DATE SIGNED

Hermann Habermann — 12/18/06

Hermann Habermann
Date

Chair, Data Stewardship Executive Policy Committee