# Polices And Procedures For Breach Notification at The U.S. Census Bureau

Mary B. Frazier, 4600 Silver Hill Road Suitland, Maryland 20746
Nancy M. Gordon, 4600 Silver Hill Road, Maryland 20746

Paper Prepared for the Joint Statistical Meetings
August 2008

## Abstract

Upon the release of the Identity Theft Task Force's September 2006 memorandum, the Census Bureau recognized the need to strengthen its processes to address potential data breaches. Both the report of the Identity Theft Task Force and the draft OMB memorandum were used as the foundation for the enhanced policy. The Census Bureau decided to use a widely accepted model of developing a risk score based on the likelihood of the event occurring and the impact of the event, an approach that was included in the OMB memorandum. The Census Bureau incorporated an existing internal board into the revised process, the Data Stewardship Executive Policy Committee (DSEP). The DSEP reviewed the policy, and it was adopted on December 15, 2006. This paper will describe the Census Bureau's processes and its experiences since they were adopted.

**Key Words:** Confidentiality, data breach, data stewardship, privacy

The U.S. Census Bureau was an early adopter of a Breach Notification Policy, putting it into place on December 16, 2006, less than three months after the Administration's Identity Theft Task Force issued its recommendations.[1] While the implementation guidelines for the policy have been updated, the policy and the core components of the guidance continue to be viable a year and a half later.

[1] A breach is defined as the 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. The breach notification policy is activated when an event suggests that a potential breach may have occurred. That policy can be found at http://www.census.gov/privacy/files/data_breach/DataBreachPolicySigned.pdf .

The Census Bureau attributes this success to several factors: a strong and long-standing commitment to data stewardship; the existence of a Privacy Office, where privacy issues are centralized; and executive level involvement and support for privacy issues, which is demonstrated by the organizational positioning of that office within the Census Bureau.

This paper elaborates on those factors and describes the next steps being planned for the Breach Notification Policy and its associated practices. Issues related to the current handling of potential breach incidents are also discussed.

## 1. BACKGROUND

This section covers the foundation of the Census Bureau's Data Stewardship program, the process by which the Privacy Office was created, and organizational support for privacy issues.

### *1.1 Data Stewardship*

The U.S. Census Bureau's senior management established the Data Stewardship Executive Policy Committee (DSEP) in 2001, to serve as the focal point for decision-making and communication on policy issues related to privacy, security, confidentiality, and administrative records. The DSEP is chaired by the Census Bureau's Deputy Director and is composed of executives who are most integrally involved in data collection, processing, analysis, dissemination, and protection. As such, the DSEP acts on behalf of senior management in developing new policy and making decisions on matters that involve these issues.

The mission of the DSEP is to ensure that the Census Bureau can effectively collect and release data about the nation's people and economy, while fully meeting the Census Bureau's legal and ethical obligations to respondents to respect their privacy and protect their confidentiality. Doing so includes fully meeting the legal, ethical, and reporting obligations levied by the Census Act (Title 13, U.S. Code), the Privacy Act, and other applicable statutes, including those of governmental and other suppliers of data to the Census Bureau.

Two standing committees report to the DSEP. Each one has a charter, an appointed Chair, and a set membership. The first – the Disclosure Review Board (DRB) – supports the Census Bureau in its efforts to protect respondents' confidentiality by adopting disclosure avoidance policies and statistical methodologies and by reviewing products (such as microdata and tables) that are to be made available to the public to protect against potential disclosures.

The second committee is the Privacy Policy and Research Committee (PPRC), which is chaired by the Chief Privacy Officer (CPO). The role of this committee is

to identify emerging policy issues, develop research agendas about them, and make recommendations to the DSEP about privacy and confidentiality issues. The committee provides a mechanism for the Census Bureau to have consistent policies on privacy protection.

### *1.2 Privacy Office*

In response to increasing concern by government officials and private groups that public agencies demonstrate their commitment to securing sensitive data, the Census Bureau initiated a program to ensure the consistent and effective treatment of privacy-related activities. The DSEP directed the PPRC to examine existing organizational structures within and outside of government to determine the value and appropriateness of establishing a Privacy Office and/or Privacy Officer for the Census Bureau.

The business case identified a variety of options and the staff tasked with developing the business case conducted interviews with leading privacy analysts in both the corporate and government sectors. Key factors considered in reaching the recommendation to establish a Chief Privacy Officer position and a Privacy Office included: the reporting level, placement of the office within the Census Bureau's structure, and its authority. In 2005, the DSEP reviewed the business case and concurred with that recommendation.

The Operating Committee concluded that the Privacy Office should report to the Deputy Director, who chairs the DSEP. The CPO sits on the DSEP to ensure that privacy issues are fully considered. Additionally, the CPO is a member of the IT Governing Board to ensure privacy issues are taken into account from the inception of IT projects.

### *1.3 Organizational Elements*

One factor contributing to the Census Bureau's success in responding to the Office of Management and Budget's (OMB's) breach notification requirements is the consolidation of responsibility for privacy issues into one office. This centralization ensures that privacy-related concerns are addressed consistently throughout the agency. This approach was validated by a recent General Accountability Office report (May 2008) that concluded that establishing a single office with responsibility for privacy-related requirements was necessary to provide consistent privacy protections.

The Privacy Office was not placed in the Information Technology (IT) Directorate so it would be better able to take a broad corporate view that includes legal and ethical considerations rather than focusing primarily on IT operations. While the Office of the Chief Information Officer (CIO) ensures that information systems and applications meet all IT security requirements including those identified in the Federal Information Security Management Act (FISMA), not all privacy issues can be addressed through IT security. Separating privacy from IT means that issues such as the public's expectations of privacy, perceptions of intrusion, and

requirements for informed consent can be addressed more directly.

The Privacy Office works closely with the Office of the CIO and the IT Security Office to ensure that technology is used to enhance privacy and does not accidentally erode it. Having the CPO serve on the IT Governing Board means that privacy issues are addressed at the earliest stages of planning and implementation of IT systems.

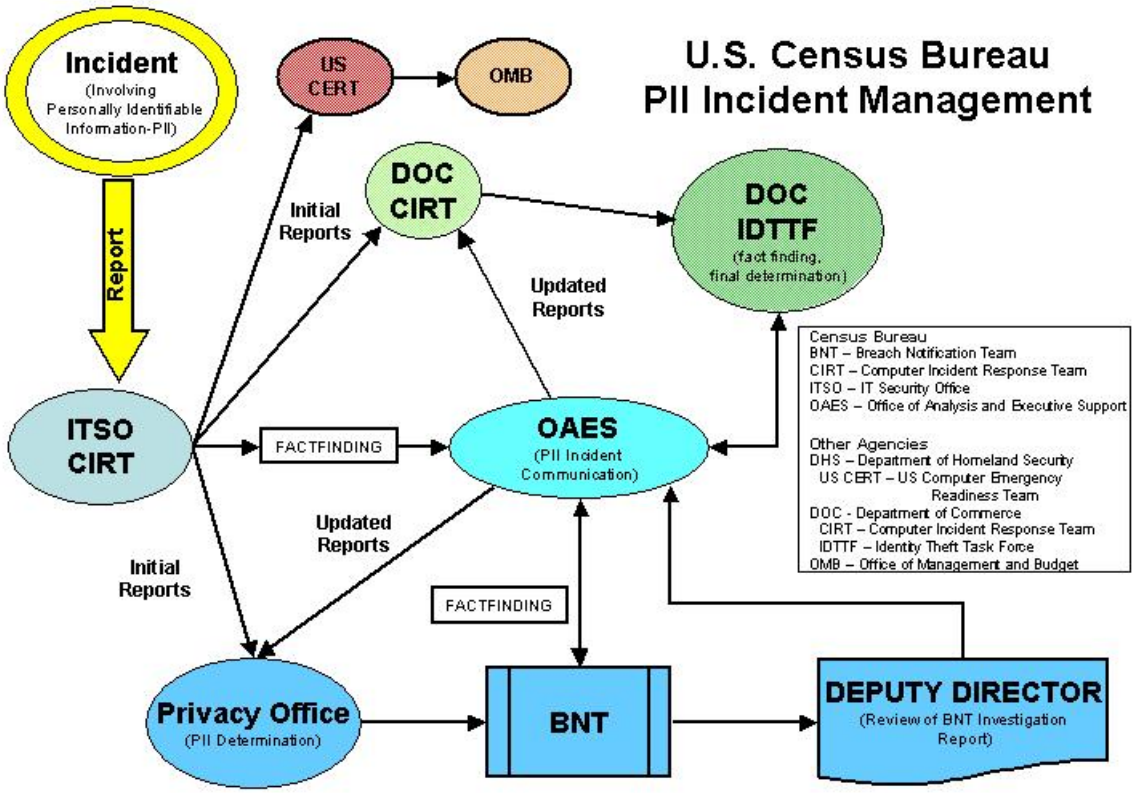
Finally, the Privacy Office works closely with the Office of Executive Analysis and Support (formerly the Policy Office) and the Office of the General Counsel. Doing so helps keep privacy activities aligned with the Census Bureau's policy and legal requirements.

## 2. CENSUS BUREAU'S BREACH NOTIFICATION POLICY

With the Privacy Office in place, the Census Bureau was able to respond immediately to the memorandum released by the Administration's Identity Theft Task Force (September 20, 2006) regarding planning for and responding to potential data breaches. The DSEP approved the plan developed by the Privacy Office and the Census Bureau had its Breach Notification Policy and associated Implementation Guide in place by December 15, 2006.

The Implementation Guide was refined and republished in October 2007, to incorporate further guidance from the OMB and practical experience gained since the first implementation in January 2007. The Department of Commerce's (DOC's) Breach Notification Response Plan, also released in October of 2007, outlined communication requirements for its bureaus and the Census Bureau modified its internal communication practices to accommodate the DOC's needs.

The Census Bureau's Breach Notification Policy incorporates the OMB requirements (released in Memorandum 07-16 on May 22, 2007) for assessing incidents and uses a Low, Medium, or High rating to determine appropriate responses. The process used by the Census Bureau provides consistent assessments of similar incidents but is flexible enough to handle anomalies and unusual cases. The team that assesses an individual incident includes the senior managers with responsibility for the organizational area in which the incident occurred, which ensures that the handling of incidents receives attention at the highest levels within the agency. The chart shows how organizational units at the Census Bureau and the DOC currently handle a potential breach, including reporting it to the U.S. Computer Emergency Readiness Team (US CERT) in the Department of Homeland Security (DHS) and the OMB.




## 3. MOVING FORWARD

This section discusses the Census Bureau's experience to date and how it will be used for future improvements.

### *3.1 Lessons Learned*

The Census Bureau's experience during the past eighteen months has provided valuable insights into different situations and types of incidents. That experience is enabling the Census Bureau to assess ways to update the mechanism for dealing with incidents, in order to better align the responses to the circumstances of the incidents, and thereby to develop more consistent assessments. While the OMB guidance provides an excellent starting point, the Census Bureau has found that some elements of the risk matrix need to be more concisely defined and new elements need to be added. For example, the Census Bureau is adding queries that pertain to items like badges (such as whether they are tamper-proof). Additional considerations include whether a loss was confined to secure government facility space or occurred elsewhere.

The tracking and review of incidents has also revealed recurring scenarios. The Census Bureau has been able to standardize its response to some of them, thus streamlining its handling practices. More important, the identification of these

scenarios provided an impetus for investigating alternative ways to reduce the risk of their occurring in the future.

### *3.2 Interactions with Other Federal Agencies*

Maturity of the breach notification activities of other agencies, and implementation of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) for protection of data, require the development of new language in interagency agreements for reimbursable work like data collection and for the acquisition of data such as administrative records. For example, the division of responsibility for breach notification for joint activities needs to be determined. Factors to be considered include the laws and regulations protecting the data, the perspective of the individual who may be affected by an incident, and the impact on all involved agencies, including costs, productivity, and the ability to achieve their missions.

## 4. CONCLUSION

The Census Bureau is not alone in trying to address issues related to handling potential breach incidents. As part of the federal statistical system, we want to work closely with the other agencies to address common situations involving statistical data in a consistent manner, while retaining the flexibility to handle unique situations appropriately. Innovative solutions for such issues often result from activities such as meetings of the Privacy Subcommittee of the Federal Committee on Statistical Methodology (FCSM), and we encourage other agencies to continue to participate in that forum.