DATA BREACH POLICY IMPLENTATION GUIDE

OCTOBER 15, 2007

Enclosure 4

Data Breach Policy Implementation Guide

Purpose

The response to any breach of personally identifiable information (PII) can have a critical impact on the U.S. Census Bureau's reputation and how trustworthy the public perceives the agency. Thus, exceptional care must be taken when responding to data breach incidents. Not all incidents result in data breaches, and not all data breaches require notification. This guide is to assist the Data Breach Team in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Background

This Data Breach Policy Implementation Guide is based on the President's Identity Theft Task Force recommendations that provide a menu of steps for an agency to consider, so that it may pursue a risk-based, tailored response to data breach incidents. Ultimately, the precise steps to take must be decided in light of the particular facts presented, as there is no single response for all breaches. Please refer to the Identity Theft Task Force Memorandum document entitled *Identity Theft Related Data Security Breach Notification Guidance* dated September 19, 2006 for additional insight and assessment considerations. Further guidance can be obtained in the NIST Special Publication 800-16, *Computer Security Incident Handling Guide.*

A. What constitutes a breach?

A breach is a 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 PII in usable form, whether physical or electronic.

B. How is a potential breach reported?

- Breaches are reported immediately through the Census Bureau Computer Incident Response Team (CIRT).
- Census CIRT procedures are available at: http://cww2.census.gov/it/itso/itso_incident_reporting.asp
- The IT Security Office (ITSO) Computer Incident Response Team (CIRT) in conjunction with the Network Operations Center (NOC) within the Bowie Computer Center have established a toll-free number to report the actual or suspected loss of sensitive data. The number (**877-343-2010**) provides Field Representatives and other employees a 24-hour contact channel to use when reporting loss or theft of sensitive data, regardless of media.
- Breaches or improper disclosures of Title 26 federal tax information (FTI) must be reported upon discovery by the individual making the observation to the Treasury inspector General for Tax Administration at 1-800-366-4484. The Data Breach Team should establish communications with the reporter of such breaches to determine appropriate actions.

C. How is a breach identified?

- A weekly review of all incidents reported through the CIRT can determine which ones should be investigated as breaches. At a minimum, the Chief Privacy Officer (CPO), Chief Information Officer (CIO), and Chief, IT Security Office should review incidents and provide a report to the Senior Agency Official who can then certify those incidents that don't warrant investigations as breaches.

D. Who gets involved in Breach Response?

1. Senior Agency Official – Director or Deputy Director
2. Chief Privacy Officer (CPO)
3. Chief Information Officer (CIO)
4. Chief, IT Security Office (ITSO)
5. Associate Director for Communications
6. Chief, Office of Analysis and Executive Support (OAES)

As warranted:

7. Chief, Office of Security
8. General Counsel
9. Inspector General
10. Law Enforcement

Risk Assessment

A. Assessing risk and harm to organization and individuals

Risk is a function of the probability or likelihood of a privacy violation, and the resulting impact of that violation. To assign a risk score, assess the probability of the event (data breach) occurring and then assess the impact or harm caused to an individual and our organization in its ability to achieve its mission.

Table 1. Likelihood Definitions

Likelihood	Likelihood Definition
High (H)	The nature of the attack and the data indicate that the motivation is criminal intent; the security of the data and controls to minimize the likelihood of a privacy violation are ineffective.
Medium (M)	The nature of the attack and data indicate that the motivation could be criminal intent; but controls are in place that may impede success.
Low (L)	The nature of the attack and data do not indicate criminal intent, and security and controls are in place to prevent, or at least significantly impede, the likelihood of a privacy violation.

To assess likelihood of a breach occurring, consider five factors:

1. How the loss occurred
2. Data elements breached
3. Ability to access the data - the likelihood the personal information will be or has been compromised – made accessible to and usable by unauthorized persons
4. Ability to mitigate the risk of harm
5. Evidence of data being used for identity theft or other harm

1. How Loss Occurred
   - H - Online system hacked
   - H - Data was targeted
   - M - Device was targeted
   - M - Device stolen
   - L - Device lost

2. Data Elements Breached*
   - H - Social Security Number
   - H - Biometric record
   - H - Financial account number
   - H - PIN or security code for financial account
   - H - Health data
   - M - Birthdate
   - M - Government Issued Identification Number (drivers license, etc.)
   - L - Name
   - L - Address
   - L - Telephone Number

*A combination of identifying information and financial or security information should always be considered a high risk with high likelihood of harm occurring.

3. Ability to access data
   - H – paper records or electronic records in a spreadsheet that is not password protected
   - M – electronic records that are password protected only
   - L – electronic records that are password protected and encrypted

4. Ability to mitigate the risk of harm
   - H – no recovery of data
   - M – partial recovery of data
   - L – recovery of data prior to use

5. Evidence of data being used for identity theft or other harm
   - H – Data published on the web
   - M – Data accessed but no direct evidence of use
   - L – No tangible evidence of data use

After evaluating each factor and assigning an overall probability or likelihood of a breach occurring, review and assess the impact or harm to an individual or our organization.

Table 2. Impact Rating Definitions

Impact Rating	Impact Definition
High	Event (1) may result in human death or serious injury or harm to individual; (2) may result in high costs to organization; or (3) may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	Event (1) may result in injury or harm to the individual; (2) may result in costs to the organization; or (3) may violate, harm, or impede an organization's mission, reputation, or interest.
Low	Event (1) may result in the loss of some tangible organizational assets or resources; or (2) may noticeably affect an organization's mission, reputation, or interest.

The impact depends on the extent to which the breach poses a risk of identity theft or other substantial harm to an individual such as: embarrassment, inconvenience, unfairness, harm to reputation or the potential for harassment or prejudice, particularly when health or financial benefits information is involved (5 U.S.C. § 552a (e)(10)).

Financial considerations can be factored in when determining the impact on our organization. For instance, credit monitoring is generally estimated at $20 per year per case (individual). The costs associated with implementing a call center including staff salaries may also be a factor. Alternatively, the cost of contracting for this service could be a factor.

B. Assigning Risk Score

The risk score is determined by cross-referencing the likelihood score with the impact score.

Table 3. Risk Scores

Likelihood	Impact		
	Low	**Medium**	**High**
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

Notification

A. If, when, and how are individuals notified?

The risk score assigned will help determine if and when we should provide notification. If the likelihood of risk is low, there could be more harm or impact on the individual if notification is provided due to the actions the notified individual may take. Thus, notification must be weighed with the likelihood of risk. No notification may be required when the risk levels of each of the five factors is low. If the likelihood of risk is high and the level of impact or harm to the individual is medium, notification and remedy may be required. Alternatively, if the likelihood of risk is low and the level of impact or harm to the individual is high, notification only may be required. If the five factors are considered appropriately, it is more likely that notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification and thus the associated further complications to the individual.

Thus, consideration should be given to all factors when determining final actions to take when addressing each incident. The table below should only be used as guide and conditions may warrant actions above or below those associated with the final risk score.

Table 4. Action

Risk Score	Necessary Action
High	Notify and provide remedy
Medium	Notify only
Low	Monitor only

B. When are they told?

Notice will be provided within a reasonable time following the discovery of a breach consistent with the legitimate needs of law enforcement and national security and any measures necessary for the Census Bureau to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the system/process that was compromised.

In some circumstances, law enforcement or national security considerations may require a delay in notification if the investigation of the breach or of an individual affected by the breach requires it and notification would seriously impede the investigation. The delay should not exacerbate risk or harm to any affected individual(s) or be tied to the completion of the investigation, but rather be based on whether it would seriously impede the investigation to provide the notice promptly.

C. Who tells them?

The notice should come from the Senior Agency Official. If the breach involves a Federal contractor or public-private partnership, the Census Bureau response will consider the specific relationship and any signed agreements.

D. What are they told?
The notice must be clear, concise, conspicuous, easy-to-understand, in plain language and should include the following elements:

- A brief description of what happened, including the date(s) of the breach and its discovery.
- A description of the types of personal information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.) to the extent possible.
- What steps, if any, an individual should take to protect himself from potential harm.
- What the Census Bureau is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches.
- Who and how affected individuals should contact the Census Bureau for more information, including a toll-free telephone number, e-mail address, and postal address.
- Direction to additional guidance available from the Federal Trade Commission at: http://www.consumer.gov/idtheft/.
  Minimizing your risk at: http://www.consumer.gov/idtheft/con_minimize.htm.
  Publications at: http://www.consumer.gov/idtheft/con_pubs.htm.

E. How are they told?
Notice of the breach will be provided commensurate to the number of individuals affected by the breach and the availability of contact information the Census Bureau has for the affected individuals. Correspondence must be prominently marked on the exterior reflecting the importance of the communication to help ensure the recipient does not discard or otherwise ignore the notification.

- In general, the primary means of notification will be by first-class mail to the last known mailing address of the individual based on Census Bureau records.

- Where we have reason to believe that the address is no longer current, reasonable efforts will be made to update the address using the U.S. Postal Service National Change of Address (NCOA) database.

- Substitute notice **may** be made in instances where the Census Bureau does not have sufficient contact information for those who need to be notified. In such instances, notice **may** consist of a conspicuous posting of the notice on the Census Bureau's home page of its web site and include additional information in a Frequently Asked Questions (FAQ). Notification **may,** if deemed necessary, be provided to major print and broadcast media in areas where the affected individuals reside. The notice to media, if warranted, will include a toll-free phone number where an individual can learn whether his or her personal information was included in the breach.

- Special consideration will be given in providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the Census Bureau web site.

Remedy

A. If, when and how is remedy provided?
Remedy is provided when the risk score is High. The easiest method is to use the GSA Blanket Purchase Agreement (BPA) # 10266. Federal Supply Schedule BPAs eliminate contracting and open market costs such as the search for sources, the development of technical documents and solicitations, and the evaluation of offers. This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from Financial and Business Solutions (FABS) Schedule contracts. The end-result is a purchasing mechanism for the Government that works better and costs less. This BPA provides multiple levels of service from three companies:

- GS-23F-06-E3-A-0013 Bearak Reports (Woman-Owned, Small)
- GS-23F-06-E3-A-0014 Equifax Inc. (Large)
- GS-23F-06-E3-A-0015 Experian Consumer Direct (Large)

Each company offers three basic levels of service. The nature of the breach, including the data and number of individuals, should be considered when deciding the service to provide. Additionally, if the event warrants it, optional supplemental services can be procured.

See attachment for additional details on services.

Data Breach Team Follow-up

The Data Breach Team will file a report identifying the Risk Score associated with the incident and the follow-up action or response they took.

The Data Breach Team will file all documents (emails, letters, Request for Quotes, etc.) created in response to the incident in a secure location that is accessible to all Data Breach Team members to use in responding to any future incidents.

Attachment

Bearak Reports Credit Monitoring Data Breach Risk Packages

Low Risk Package	**Low Risk Package Includes:** ▪ Social Security, Credit Card and 1 Bureau Credit Report Monitoring ▪ 3 Bureau Initial Fraud Alert ▪ Credit Card Registry ▪ Online Identity Theft Assistance ▪ 24 x 7 Customer Support
Medium Risk Package	**Medium Risk includes Low Risk benefits plus:** ▪ Instant 1 Bureau Credit Report ▪ Instant 1 Bureau Credit Score ▪ Personal Information Directory Monitoring and Deletion ▪ Identity Theft Consumer Guide ▪ $25,000 ($0 deductible) Identity Theft Insurance
High Risk Package	**High Risk includes Medium Risk benefits plus:** ▪ 3 Bureau Credit Report Monitoring ▪ Instant 3 in 1 Credit Report ▪ Instant 3 Bureau Credit Scores ▪ Fraud Resolution & Identity Restoration Specialist

Equifax Credit Monitoring Services

Features/Functionality	Silver (Good)	Gold (Better)	Gold with 3-in-1 Monitoring (Best)
Product Type	One Year Membership Service		
Enrollment Method	Internet	Internet, Fax, US Mail	
Access Method	Internet	Internet or US Mail	
Alert Frequency	Weekly	Daily	
Alert Method	Internet & Wireless Devices	Internet & Wireless Devices or US Mail	
Alert Types	▪ New Credit Inquiries ▪ New Accounts Established ▪ Name/Address Changes ▪ New & Changes to Public Records (bankruptcy, collections, suits or judgments &/or liens ▪ Account Balance ($ and %) changes (Internet enrollees only) ▪ Dormant Account Activity (Internet enrollees only)		
Credit Reports	One Equifax Credit Report (Internet Delivery)	Unlimited Equifax Credit Reports (Internet Delivery)	One 3-in-1 Credit Report & Unlimited Equifax Credit Reports (Internet Delivery)
	US Mail delivery is NOT AVAILABLE	One Equifax Credit Report at enrollment with Quarterly updates (US Mail delivery)	One 3-in-1 Credit Report at enrollment with Quarterly updates to the Equifax credit file (US Mail delivery)
Identify Theft Insurances	$2,500 with $250 deductible	$20,000 with $0 deductible	
Customer Care	Assist consumers during/after enrollment: ▪ Respond to product questions ▪ Assist in initiating dispute resolutions & ▪ Provide fraud victim assistance if consumer's identity is believed to be compromised		

Experian Credit Monitoring Services

Triple Alert℠ Monitoring – This product is delivered to qualified* Individuals using an online or offline application process and a single-use, Access Code.	**Triple Alert benefits include:** ▪ Automatic daily monitoring of credit reports from all three national credit reporting companies: Experian, Equifax and TransUnion ▪ Email or US mail monitoring alerts to inform the Individual of key changes to their credit reports, including new inquiries, newly opened accounts, delinquencies, address changes and public record items ▪ Monthly "no hit" alerts, if there have been no important changes to the Individual's credit report ▪ Informative credit related articles ▪ Toll-free Customer Service ▪ Toll-free access to fraud resolution representatives and support should the Individual become a victim of Identity Theft after s/he enrolls in Triple Alert ▪ Assistance from fraud resolution representatives who will walk the Individual step-by-step through the process of resolving problems associated with credit fraud or Identity Theft and: (i) assist with understanding credit reports and alerts (ii) assist in contacting law enforcement officials, (iii) receive and make calls with the Individual, and (iv) contact financial institutions and creditors as required. All assistance is provided as appropriate on a case by case basis ▪ $10,000 or $25,000 identity theft insurance coverage provided by a designated third party insurer
Triple Advantage℠ Monitoring (Premium) –This product is delivered to qualified* Individuals using an online or offline application process and a single-use, Access Code.	**Triple Advantage benefits include:** ▪ Automatic daily monitoring of credit reports from all three national credit reporting companies: Experian, Equifax and TransUnion ▪ Email or US mail monitoring alerts to inform the Individual of key changes to their credit reports, including new inquiries, newly opened accounts, delinquencies, address changes and public record items ▪ Monthly "no hit" alerts, if there has been no important changes to the Individual's credit report ▪ Unlimited online and offline access to the Individual's Experian® Credit Report and Score for the duration of the membership ▪ Score Simulator - helps Individuals understand how factors on their credit report impact their credit score ▪ Consumer-friendly credit report with detailed explanations and descriptions ▪ Monthly Score Trending of the Individual's Experian score ▪ Informative credit related articles ▪ One free 3 bureau Credit Report and score upon enrollment ▪ Toll-free Customer Service ▪ Toll-free access to fraud resolution representatives and support should the Individual become a victim of Identity Theft after s/he enrolls in Triple Advantage ▪ Assistance from fraud resolution representatives who will walk the Individual step-by-step through the process of resolving problems associated with credit fraud or Identity Theft and: (i) assist with understanding credit reports and alerts (ii) assist in contacting law enforcement officials, (iii) receive and make calls with the Individual, and (iv) contact financial institutions and creditors as required. All assistance is provided as appropriate on a case by case basis ▪ $25,000 identity theft insurance coverage provided by a designated third party insurer