General Guidance for the Establishment of a Toll-Free Number or Call Center in the Event of a Privacy Act Breach

In the event of a privacy breach or spillage of Personally Identifiable Information (PII) the following guidance is provided as the command considers whether to establish a call center to handle inquiries related to the incident. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the spillage and possible actions they may want to take to lessen the incident's impact on their personal lives (i.e., identity theft, etc.).

The decision to establish a call center should be based on several considerations:

- If a command has a privacy breach that does not extend outside the organization (i.e., those affected by the breach are known and can be contacted), then establishment of a call center would not normally be necessary.

- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted (e.g., "all surface line officers since 1970"), establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach.

- Each situation will be unique and the decision to establish a call center must be based on the individual circumstances. The main concern should be the sharing of information with those affected and how they may obtain assistance.

Once the decision is made to establish a call center there are several options:

- Contact your local service provider (AT&T, Sprint, Verizon, etc.) to obtain a toll-free number. The provider's website under their business or government services area, in many cases, can provide information regarding who to contact, features, costs, etc. This option is most likely the least expensive, since you will be providing your own manning.

- Contact the General Services Administration's (GSA) USA Services Group to establish a call center supported and manned by GSA personnel. A statement of work (SOW) will be required and the call center can be up and running usually within 72 hours. SOW requirements can be found at http://www.usaservices.gov under FirstContact. A generic SOW is provided there. A thorough description of the incident and set of frequently asked questions will also be required for GSA personnel to refer to when fielding questions. GSA POCs are: Ms. Teresa Nasif at 202-501-1794 and Mr. Bob Corey, Contracting Officer, at 202-501-1797.

Suggested items to consider based on the nature of the breach would include but are not limited to:

- Use of existing command personnel to man the call center and the number of individuals required.

- Training of call center operators.

- Pre-staged frequently asked questions (FAQS). Attached are questions used during the Veteran's Administrations privacy breach in May 2006. These could be used as a starting point and tailored to meet the requirements of a specific breach.

- Ability to adjust manning in response to call volume.

- Daily hours of operation.

- Cost of service.

- Logging calls.

- Command and higher headquarters reporting requirements.

- Advertising call center number(s) and making breach information readily available to those affected (i.e., on command's and other appropriate websites, mass emailing(s) to those affected, news media, etc.).

- Command periodic check of call center quality of customer service.

- Criteria to disestablish call center.

Sample Frequently Asked Questions:

1- How can I tell if my information was compromised?

At this point there is no evidence that any missing data has been used illegally. However, the Department of _____ is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

2- What is the earliest date at which suspicious activity might have occurred due to this data breach?

The information was stolen from an employee of the Department of _____ during the month of _____, 2006. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious

activity during the month of _____.

3- I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

The Department of _____ strongly recommends that individuals closely monitor their financial statements and visit the Department of _____ special website at www._____.gov.

4- Should I reach out to my financial institutions or will the Department of _____ do this for me?

The Department of _____ does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

5- Where should I report suspicious or unusual activity?

The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

Step 1 – Contact the fraud department of one of the three major credit bureaus:

> Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
>
> Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013.
>
> TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

Step 2 – Close any accounts that have been tampered with or opened fraudulently.

Step 3 – File a police report with your local police or the police in the community where the identity theft took place.

Step 4 – File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by telephone: 1-877-438-4338, online at www.consumer.gov/idtheft, or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

6- I know the Department of _____ maintains my health records electronically. Was this information also compromised?

No electronic medical records were compromised. The data lost is primarily limited to an individual's name, date of birth, social security number, in some cases their spouse's information, as well as some disability ratings. However, this information could still be of potential use to identity thieves and we recommend that all veterans be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

7- What is the Department of _____ doing to insure that this does not happen again?

The Department of _____ is working with the President's Identity Theft Task Force, the Department of Justice and the Federal Trade Commission to investigate this data breach and to develop safeguards against similar incidents. The Department of _____ has directed all employees to complete the "VA Cyber Security Awareness Training Course" and complete the separate "General Employee Privacy Awareness Course" by _____, 2006. In addition, the Department of _____ will immediately be conducting an inventory and review of all current positions requiring access to sensitive data and require all employees requiring access to sensitive data to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the Federal Bureau of Investigation and the Inspector General of the Department of _____, have launched full-scale investigations into this matter.

8- Where can I get further, up-to-date information?

The Department of _____ has set up a special website and a toll-free telephone number for employees which features up-to-date news and information. Please visit www._____.gov or call 1-800-XXX-XXXX.

9- Does the electronic data theft affect only _____?

It potentially affects all employees hired since _____, which is when automated records management began and regular input of information commenced.

We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.