Responding to the Public after a Breach of Personal Information: Government Actions & Lessons Learned

Information **S**ecurity and
Privacy **A**dvisory **B**oard Meeting

September 15, 2006

Teresa Nasif
Executive Sponsor, USA Services
Office of Citizen Services & Communications
U.S. General Services Administration

E·GOV

USA Services

- Who We Are; What We Do….
- Our role in Federal response to stolen VA computer incident
- Lessons Learned

USA Services

May 3, 2006:

- A computer is stolen with Department of Veterans Affairs sensitive data
- Action of one VA employee affects 26.5 million veterans and dependents

USA Services

May 19th, 4:00 pm:

I received a late Friday afternoon call at USA Services from the VA:

- The following Monday, there will be a press conference announcing the theft of a government laptop from an employee's home
- 26.5 million veterans and dependents would want to call someone about the matter

USA Services

- USA Services is a Presidential e-gov initiative that helps government be more citizen-centric
- We provide direct service to citizens via:
  - -- FirstGov.gov site
  - -- 1-800 FED INFO
  - -- E-mail
  - -- Pueblo
- We help agencies respond to the public more efficiently and effectively, in everyday situation or in response to emergencies
- Direct outgrowth of USAS was the creation of the FirstContact contract

USA Services

- Proven track record in responding to citizen phone calls and e-mails in times of disaster
- USA Services helps agencies cope with the aftermath
- Have handled broad range of government calls for decades
- After 9/11, began handling calls for State Department for overseas citizens

USA Services

FirstContact offers:

- Pool of 5 pre-qualified contact center vendors
- “The Five” offer a wide range of services at a “best in industry” level of performance
- Experienced GSA staff will shepherd agencies through the selection process

USA Services

Whether it's human nature or Mother Nature:

- After Hurricane Katrina (and Rita and Wilma), we used FirstContact to help FEMA answer calls from victims.
- Two vendors selected who managed multiple centers for three months
- Handled 1.5M calls
- When the VA laptop was stolen, OMB's Karen Evans recommended use of USAS

USA Services

May 20th -- May 22nd:

- Friday May 19th: I received the first phone call on the VA incident
- Saturday May 20th: USA Services awards the task order
- Sunday May 21st: White House meeting to map strategy and coordinate response: Karen Evans from OMB, and senior officials from VA, Justice, FBI, FTC, and USA Services.

USA Services

May 20th -- May 22nd:

- Sunday, May 22nd: Our website, Firstgov.gov, establishes a prominent link from its homepage to one exclusively for the VA incident, housing a series of FAQs. This page will be updated as the situation develops.
- In the weeks to follow, this site will experience over one million page views.
- Both the public and the agents staffing phones will use this site to answer questions.

USA Services

May 20th -- May 22nd:

- Sunday, May 22nd: Hiring begins….and is completed. Our vendors have a ready pool of phone agents.
- Monday morning, May 22nd: 1,500 agents in 6 Teletech centers and 7 ICT centers, as well as our own National Contact Center, receive training to begin answering questions from a very worried public.

USA Services

Monday, noon, May 22nd:

- Secretary Nicholson holds press conference announcing the stolen computer incident
- The media promotes the story, prominently offering 1-800 FED INFO and FirstGov.gov for more info
- Our agents are in place when the phones begin ringing

Associated Press
May 23, 2006

Data of 26.5 million veterans swiped in theft

By Hope Yen
The Associated Press

WASHINGTON — Personal data, including Social Security numbers of 26.5 million U.S. veterans, was stolen from a Veterans Affairs employee this month after he took the information home without authorization, the department said Monday.

Veterans Affairs Secretary Jim Nicholson said there was no evidence so far that the burglars who struck the employee's home have used the personal data — or even know they have it. The employee, a data analyst whom Nicholson would not identify, has been placed on leave pending a review.

"We have a full-scale investigation," said Nicholson, who said the FBI, local law enforcement and the VA inspector general were investigating. "I want to emphasize, there was no medical records of any veteran and no financial information of any veteran that's been compromised."

"We have decided that we must exercise an abundance of caution and make sure our veterans are aware of this incident," he said in a conference call with reporters.

The theft of veterans' names, Social Security numbers and dates of birth comes as the department has come under criticism for shoddy

See Veterans, Page A5

FOR MORE INFORMATION

Veterans suspecting identify theft can visit **www.firstgov.gov** or call (800) FED-INFO.

FRONT PAGE

AP photo/Lawrence Jackson

Veterans Affairs Secretary James Nicholson, right, and Attorney General Alberto Gonzales discuss Monday the theft from a VA employee's home of personal information of 26.5 million U.S veterans.

USA Services

Some of the questions the Vets asked:

- Was my information in the stolen data?
- Will my benefits be affected?
- What were the intentions of this employee?
- Does VA have a copy of the disk with the stolen records?
- When will I be notified if my information was stolen?
- Will I be held responsible for fraudulent acts in my name?
- Will the VA pay for credit card identity theft monitoring?
- I'm a dependent; was my information stolen too?
- Was the stolen data encrypted?
- What's being done to prevent this from happening again?

USA Services

And some comments they gave:

- “I know it was an inside job.”
- “The employee who took the laptop home should be prosecuted.”
- “A class action suit should be brought against the government.”
- And……

USA Services

- “I can’t even walk out of Wal-Mart with a $10 CD without setting off an alarm and someone asking to see a receipt; yet this employee walks out of an office with a laptop full of sensitive information, no questions asked.”

USA Services

In summary, the Federal response, led by VA:

- Worked closely with FBI & local law enforcement officials
- Set up multiple contact centers
- Issued press releases
- Constantly updated info on va.gov, FirstGov.gov, and DoD's website, and for the contact centers

USA Services

- Placed VA program managers on-site at the centers
- Mailed letters to all veterans
- Pursued free credit monitoring service for all vets
- GSA listed credit monitoring agencies on the GSA schedule

USA Services

Biggest Challenges:

1. Staying ahead of – or just current with – the media.

2. Ensuring accurate, responsive information by contact center agents and on FirstGov.gov

USA Services

- USA Services stayed in constant communication with VA and OMB (we filed daily reports at midnight for weeks)
- Information that we furnished on behalf of the VA had the potential for far-reaching ramifications
- Info on FirstGov.gov or provided by phone agents had to be thoroughly vetted to avoid creating confusion, panic, ill-will
- For some media, these factors were less of an issue; we constantly played catch-up with the latest headlines:

USA Services

E·GOV

VA employee improperly took data home for 3 years, investigators say

Inspector general says he learned about breach through office gossip

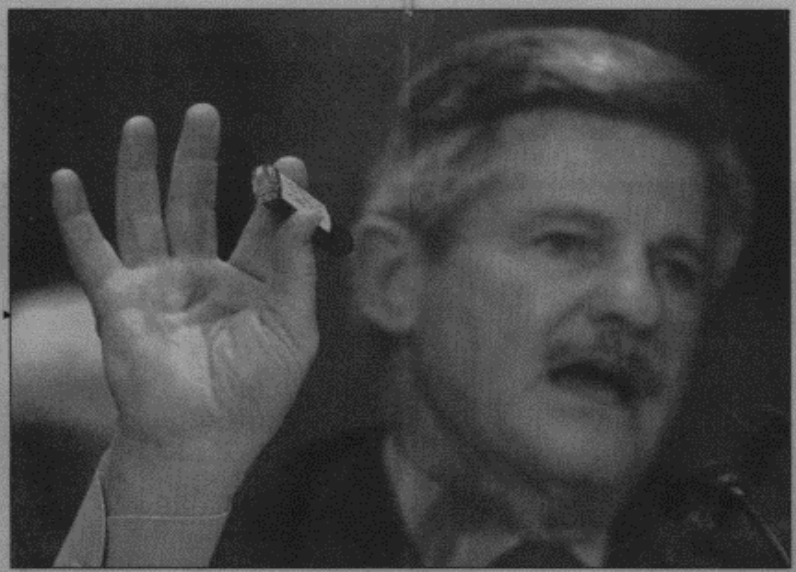
623QE

WASHINGTON (AP) — The theft of personal data for 26.5 million veterans came to the attention of the Veterans Affairs inspector general only through office gossip, he told Congress on Thursday.

In four hours of testimony, IG George Opfer said the department failed to heed years of warnings about lax security and noted that the employee who lost the data when his house was burglarized had been improperly taking the material home for three years.

"We were on borrowed time," Opfer told Senate and House panels investigating the breach.

Earlier, VA Secretary Jim Nicholson said he was "mad as hell" that he wasn't told about the burglary until May 16 — nearly two weeks after it happened. He then told the FBI on May 17, leading to a public announcement May 22.



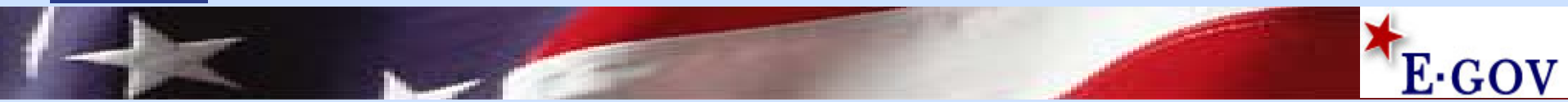
AP photo

"You seem to be saying it was just one employee. But it's not just one employee. You have a high-risk vulnerable system that has been identified time and again as vulnerable."

SEN. SUSAN COLLINS, R-MAINE,
chairwoman,
Homeland Security Committee

During the hearing Thursday, Rep Steve Buyer, R-Ind., chairman of th House veterans panel, presse Nicholson to give the nation's vete ans assurances that their informa

USA Services



Personal data of 26.5M vets stolen from VA worker

Vets With Stolen IDs Urged To Contact Feds

Identity theft may hit active duty military

Data theft gives U.S. veterans reason to worry

Theft of data shocks veterans

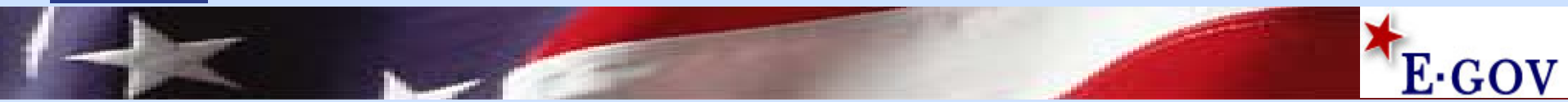
VA learned of ID theft via gossip

Frequently Asked Questions On VA's Letter To Veterans

Filner curses VA for handling of date theft

VA asking for more money to fight data theft

USA Services



Rockefeller Introduces Bill To Aid Veterans in Identity Protection

Joe wants feds to pay inVA theft

By Joseph Straw
Register Washington Bureau

Veterans warned to be on lookout for unusual financial activities, calls

Burglary leaves vets at risk for identity theft

FRONT PAGE

Secretary Nicholson Announces VA to Provide Free Credit Monitoring

ID theft protection available

Veterans advised to take steps to protect identity

Rahall: Recovery of Laptop A "Bright Spot" But Should Not Deter Mission To Protect Vets

USA Services

Nearly 700 print mentions of the data breach: FirstGov.gov and 1-800 FED INFO usually cited as a contact point for information

Data of 26.5 million veterans stolen from employee's home

BY HOPE YEN
Associated Press

623QE

WASHINGTON, D.C. | Thieves took sensitive personal information on 26.5 million U.S. veterans, including Social Security numbers and birth dates, after a Veterans Affairs employee improperly brought the material home, the government said Monday.

The information involved mainly those veterans who served and have been discharged since 1975, said VA Secretary Jim Nicholson. Data of veterans discharged be-

WHAT VETERANS CAN DO

- The VA said it is notifying members of Congress and the individual veterans about the burglary.
- The VA has set up a call center at 800-FED-INFO and a Web site, http://www.firstgov.gov, for veterans who believe their information has been misused.

USA Services

June 29, 2006:

Stolen VA laptop recovered, and not compromised.

USA Services

Lessons Learned:

- Expect an influx of public inquiries on short notice
- Work out a citizen telephone response plan that can go into effect quickly, e.g., contracting for contact center services, or marshalling agency employees
- Involve all relevant government websites
- Establish strong link between response approvers and those interacting with the public.

USA Services

Lessons Learned:

- Create swift approval process for updates to information as situation unfolds
- Ensure that all Federal information for the public is consistent no matter what the channel
- Create positive responses that agents can use even if no final decisions, or if the question is beyond scope of government responsibility (“How can I become part of a class action suit against your agency?”)

USA Services

Lessons Learned:

- Get updated information to the front lines quickly
- Have at least one agency employee onsite at each call center for knowledge support (VA did).

USA Services

Lessons Learned:

- Federal agencies: be aware that GSA has credit monitoring services on schedule now.
- http://www.gsaelibrary.gsa.gov/ElibMain/SinDetails
- General Schedule questions: 703-605-2820

USA Services

The Outcome….

- In VA's case, call response was less than expected
- 26.5M affected individuals resulted in 250,000 calls and one million page views at FirstGov.gov
- What helped:
  -- Posting info on federal websites (VA, FirstGov, DOD)
  -- Media coverage
  -- Letters to veterans

USA Services

The Outcome…

- Information on the VA laptop was not compromised, thus there was no need to offer free credit monitoring
- But it *could* have been compromised
- If VA's laptop had not been recovered, we'd have answered calls for much longer than 15 weeks

USA Services

Conclusion:

- Problem of potential data breach not limited to federal agencies: state agencies, schools, private companies are vulnerable
- Having a plan in place to respond to breaches is key to any organization that maintains sensitive data.

USA Services

USA Services

www.usaservices.gov

Teresa Nasif

202-501-1794