United States Government Accountability Office

GAO

Report to Congressional Requesters

April 2007

PRIVACY

Lessons Learned about Data Breach Notification

GAO-07-657

April 2007

PRIVACY

Lessons Learned about Data Breach Notification

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-657, a report to congressional requesters

Why GAO Did This Study

A May 2006 data breach at the Department of Veterans Affairs (VA) and other similar incidents since then have heightened awareness of the importance of protecting computer equipment containing personally identifiable information and responding effectively to a breach that poses privacy risks. GAO's objective was to identify lessons learned from the VA data breach and other similar federal data breaches regarding effectively notifying government officials and affected individuals about data breaches. To address this objective, GAO analyzed documentation and interviewed officials at VA and five other agencies regarding their responses to data breaches and their progress in implementing standardized data breach notification procedures. The cases at the other agencies were chosen because, like the VA case, they involved loss or theft of computing equipment and relatively large numbers of affected individuals (10,000 or more).

What GAO Recommends

To better ensure that individuals who are at risk of identity theft are offered consistent levels of support, GAO is recommending that the Director of OMB develop guidance for agencies on when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft. In written comments on a draft of this report, OMB and VA concurred with GAO's recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-07-657.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Based on the experience of VA and other federal agencies in responding to data breaches, GAO identified the following lessons learned regarding how and when to notify government officials, affected individuals, and the public:

- Rapid internal notification of key government officials is critical.
- Because incidents vary, a core group of senior officials should be designated to make decisions regarding an agency's response.
- Mechanisms must be in place to obtain contact information for affected individuals.
- Determining when to offer credit monitoring to affected individuals requires risk-based management decisions.
- Interaction with the public requires careful coordination and can be resource-intensive.
- Internal training and awareness are critical to timely breach response, including notification.
- Contractor responsibilities for data breaches should be clearly defined.

These lessons have largely been addressed in guidance issued in 2006 from the Office of Management and Budget (OMB), which is responsible for overseeing security and privacy within the federal government. However, guidance to assist agency officials in making consistent risk-based determinations about when to offer credit monitoring or other protection services has not been developed. Without such guidance, agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals, potentially leaving some people more vulnerable than others.

Contents

Abbreviations

HHS	Department of Health and Human Services
OMB	Office of Management and Budget
PII	personally identifiable information
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

April 30, 2007

Congressional Requesters

In May 2006, the Department of Veterans Affairs (VA) announced that computer equipment containing personally identifiable information (PII)[1] on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Until the equipment was recovered, veterans did not know whether their information was likely to be misused. In addition to concerns about protecting personal information, the incident highlighted unclear policy about security breach notification procedures. The VA data breach coupled with recent reports of other federal data breach incidents have heightened awareness of the need for agencies to be prepared to effectively respond to a breach that poses privacy risks.

While existing laws generally do not require agencies to notify affected individuals of data breaches, such notification appears to be consistent with agencies' responsibilities under the Privacy Act of 1974 and promotes accountability for privacy protection.[2] When data breaches occur, notification has clear benefits such as allowing the affected individuals the opportunity to take steps to protect themselves from identity theft or other misuse of their personal information.

However, as we noted in June 2006, public notification of data breaches presents challenges as well as benefits.[3] Determining the specific criteria for incidents that merit notification involves these important considerations:

[1]"Personally identifiable information" refers to any information about an individual maintained by an agency, including any information that 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., and any other personal information which is linked or linkable to an individual.

[2]The recently enacted Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461 requires VA to issue interim regulations for the provision of certain services, including notification, in the event a data breach of veterans' sensitive personal information results in a determination that a reasonable risk exists for the potential misuse of the information.

[3]GAO, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information*, GAO-06-833T (Washington, D.C.: June 8, 2006).

- Notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion.

- Sending too many notices, based on overly strict criteria, could render all such notices less effective, because consumers could become desensitized to them and fail to act when risks are truly significant.

- The costs associated with notification are not insignificant for either agencies or individuals.

As agreed with the requesters' staff, our objective was to identify lessons learned from the VA data breach and other similar federal data breaches regarding effectively notifying government officials and affected individuals about data breaches.

To address our objective, we analyzed documentation capturing lessons learned from VA's data breach, including reports on actions taken and planned to address the data breach and to protect personal information. We interviewed VA officials regarding how they decided to address data breach notification and their plans and progress in implementing standardized data breach notification procedures. We also analyzed current federal guidance on data breach notification procedures and interviewed cognizant officials about the guidance. In addition, we examined similar data breach cases at five other agencies—the Departments of Agriculture, Defense, Education, Health and Human Services (HHS), and Transportation—to determine their notification practices and lessons learned regarding how and when to notify affected individuals or the public. These cases were chosen because, like the VA case, they involved relatively large numbers of affected individuals (10,000 or more) and also involved circumstances similar to VA's—the loss or theft of computing equipment containing PII. The cases at Agriculture, Education, and HHS involved data breaches of information held by contractors. We conducted our review in accordance with generally accepted government auditing standards from August 2006 through February 2007.

On March 9, 2007, we provided staff of requesters with a briefing on the results of our study. The slides from that briefing, with minor technical clarifications, are included as appendix I of this report. The purpose of this report is to provide the published briefing slides to you and to officially transmit our recommendation to the Office of Management and Budget (OMB).

In summary, based on the experience of VA and other federal agencies in responding to data breaches, we identified the following lessons learned regarding how and when to notify government officials, affected individuals, and the public:

- *Rapid internal notification of key government officials is critical.* Internal delays prevented key VA officials, including the Secretary, from being aware of the data breach until as long as two weeks after it occurred. Because of these delays, the department's decision about how to respond was also delayed. As a result, affected individuals were denied the opportunity to take prompt steps to protect themselves against the dangers of identity theft. Prompt internal notification would help ensure that future data breaches are addressed promptly, maximizing the opportunity for affected individuals to effectively take precautions.

- *Because incidents vary, a core group of senior officials should be designated to make decisions regarding an agency's response.* In the VA incident, a variety of key decisions needed to be made including, what information had been compromised and what risks the theft posed, and how affected individuals should be notified. Cognizant officials at VA were initially unsure about who should be involved in decision making about the incident. Establishment of core management groups within agencies that can be convened in the event of a breach to evaluate the situation and guide the agency's response should help ensure that future data breaches are addressed consistently.

- *Mechanisms must be in place to obtain contact information for affected individuals.* VA and other agencies faced challenges in identifying addresses for all individuals affected by their data breaches. If proper public notices as required by the Privacy Act are made in advance, key agencies will more likely be in a better position to assist in responding to data breaches by providing address or other contact information to affected agencies.

- *Determining when to offer credit monitoring to affected individuals requires risk-based management decisions.* Agencies have made varying decisions about how and when to offer credit monitoring. As a result, affected individuals may not always receive a consistent level of support from the federal government when their personal information is compromised. Until guidance is available to promote consistent

decision making by federal agencies, protections offered to affected individuals are likely to remain inconsistent.

- *Interaction with the public requires careful coordination and can be resource-intensive.* VA invested substantially in facilities to help address follow-on inquiries and provide information to support affected individuals after notifications were issued to affected individuals. Other agencies have also taken a variety of actions to establish call centers to interact with the public.

- *Internal training and awareness are critical to timely breach response, including notification.* The slow response to the May 2006 VA incident highlighted the need for personnel to be more aware of the agency's privacy and security procedures, including incident response and reporting procedures. Because a prompt response is critical, agency personnel must be prepared in advance with an understanding of their roles and responsibilities in responding to a data breach.

- *Contractor responsibilities for data breaches should be clearly defined.* While the VA data breach did not involve contractors, the issue of contractor responsibilities has figured prominently in three other recent incidents (at Agriculture, Education, and HHS). Contractor obligations for taking steps, such as notifying affected individuals or providing credit monitoring, may be unclear unless specified in the contract.

These lessons have largely been addressed in guidance from OMB, which is responsible for overseeing security and privacy within the federal government. However, guidance to assist agency officials in making consistent risk-based determinations about when to offer credit monitoring or other protection services has not been developed. Without such guidance, agencies could make inconsistent decisions about what protections to offer affected individuals, potentially leaving some more vulnerable than others.

Conclusions

VA's data breach of May 2006 and other recent federal data breaches provide valuable lessons learned for agencies about responding to such incidents. Key government officials need to be informed promptly, and a designated group of agency officials must be ready to make prompt decisions about notification, which can be challenging if address information is not readily available. Careful planning is needed to be able to

interact effectively with the public, training and awareness are critical, and contractor roles and responsibilities must be defined.

To its credit, OMB responded to the VA data breach by issuing guidance and forwarding recommendations by the ID Theft Task Force that largely address these lessons. However, the issue of how to make risk-based determinations on when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, has not been addressed in guidance. Without such guidance, agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals.

Recommendation for Executive Action

We recommend that the Director of OMB develop guidance for federal agencies on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a federal data breach.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from OMB Administrator of the Office of E-Government and Information Technology and from the Secretary of Veterans Affairs. (These written comments are reproduced in apps. II and III.) OMB agreed with our recommendation and noted that while it is important that individuals receive consistent responses and levels of support from federal agencies, the same response or type of support will not be appropriate in every situation. We agree that appropriate responses must be tailored to address the circumstances of the breach and believe additional guidance from OMB can facilitate consistent agency decision making about such responses. In addition, OMB commented that our definition of PII is similar to one it has used and noted that its definition of PII is likely to be revised in the future. However, we believe the definition we have used is appropriate for the material discussed in this report.

In written comments on the draft of this report, the Secretary of VA agreed with our findings and our recommendation to OMB. The Secretary also stated that VA is finalizing its new data breach regulation that implements the Veterans Benefits, Health Care, and Information Technology Act of

2006, Public Law 109-461.[4] This act requires VA to issue interim regulations for the provision of certain services, including notification, in the event that a data breach of veterans' sensitive personal information results in a determination that a reasonable risk exists for the potential misuse of the information.

We are sending copies of this report to interested congressional committees; the Secretary of Veterans Affairs; the Director, OMB; and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at www.gao.gov.

Should you have any questions on matters contained in this report, please contact me at (202) 512-6240 or by e-mail at koontzl@gao.gov. GAO staff who made major contributions to this report are included in appendix IV.

Linda D. Koontz
Director, Information Management Issues

[4]Title IX of this statute contains the Department of Veterans Affairs Information Security Enhancement Act of 2006 referred to on page 1.

List of Requesters

The Honorable Harry Reid
Majority Leader
United States Senate

The Honorable Daniel K. Akaka
Chairman
Committee on Veterans' Affairs
United States Senate

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Bob Filner
Chairman
Committee on Veterans' Affairs
House of Representatives

The Honorable Hillary Rodham Clinton
United States Senate

The Honorable Byron L. Dorgan
United States Senate

The Honorable Patty Murray
United States Senate

The Honorable Barack Obama
United States Senate

The Honorable John D. Rockefeller, IV
United States Senate

The Honorable Ken Salazar
United States Senate

The Honorable Charles E. Schumer
United States Senate

Briefing to Staff of Congressional Requesters

Privacy: Lessons Learned about Data Breach Notification

Briefing to staff of Congressional Requesters

March 09, 2007

1

GAO
Accountability * Integrity * Reliability

Contents

GAO
Accountability * Integrity * Reliability

Introduction

In May 2006, the Department of Veterans Affairs (VA) announced that computer equipment containing personally identifiable information (PII)[1] on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee.

In June, VA sent notices to the affected individuals that explained the breach and offered advice on steps to take to reduce the risk of identity theft.

The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised.[2]

[1]Personally Identifiable Information refers to any information about an individual maintained by an agency, including any information that 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., and any other personal information which is linked or linkable to an individual.

[2]For detailed information about the facts and circumstances surrounding the VA data breach incident, see Department of Veterans Affairs Office of Inspector General, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, Report No. 06-02238-163 (Washington, D.C.: July 11, 2006).

GAO
Accountability * Integrity * Reliability

Introduction

Until the equipment was recovered, veterans did not know whether their information was likely to be misused.

In addition to concerns about protecting personal information, the incident highlighted unclear policy about security breach notification procedures.

The Senate Majority Leader, the Chairman, Senate Committee on Veterans Affairs, and other Congressional requesters asked us to review lessons learned from the VA data breach about how to effectively notify government officials and the public about security breaches.

Objective, Scope, and Methodology

As agreed with the requesters' staff, our objective was to identify lessons learned from the VA data breach and other similar federal data breaches regarding effectively notifying government officials and affected individuals about data breaches.

To address our objective, we

- Analyzed documentation capturing lessons learned from VA's data breach, including reports on actions taken and planned to address the data breach and to protect personal information.
- Interviewed VA officials regarding how they decided to address data breach notification and their plans and progress in implementing standardized data breach notification procedures.
- Analyzed current federal guidance on data breach notification procedures and interviewed cognizant officials about the guidance.

5

Objective, Scope, and Methodology

- Examined similar data breach cases at five other agencies—the Departments of Agriculture, Defense, Education, Health and Human Services (HHS), and Transportation—to determine their notification practices and lessons learned regarding how and when to notify affected individuals or the public. The cases were chosen because, like the VA case, they involved relatively large numbers of affected individuals (10,000 or more) and also involved circumstances similar to VA's—the loss or theft of computing equipment containing PII. The cases at Agriculture, Education, and HHS involved data breaches of information held by contractors.

We conducted our review in accordance with generally accepted government auditing standards from August 2006 through February 2007.

6

Results In Brief

Based on the experience of VA and other federal agencies in responding to data breaches, we identified the following lessons learned regarding how and when to notify government officials, affected individuals, and the public:

- Rapid internal notification of key government officials is critical.
- Because incidents vary, a core group of senior officials should be designated to make decisions regarding an agency's response.
- Mechanisms must be in place to obtain contact information for affected individuals.
- Determining when to offer credit monitoring to affected individuals requires risk-based management decisions.
- Interaction with the public requires careful coordination and can be resource-intensive.
- Internal training and awareness are critical to timely breach response, including notification.
- Contractor responsibilities for data breaches should be clearly defined.

7

Results In Brief

These lessons have largely been addressed in guidance from the Office of Management and Budget (OMB), which is responsible for overseeing security and privacy within the federal government. However, guidance to assist agency officials in making consistent risk-based determinations about when to offer credit monitoring or other protection services has not been developed. Without such guidance, agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals, potentially leaving some more vulnerable than others.

To better ensure that individuals who are at risk of identity theft are offered consistent levels of support, we are recommending that the Director, OMB, develop guidance for agencies on when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a federal data breach.

8

Results In Brief

An OMB Policy Analyst in the Information Policy and Technology Branch provided an e-mail message stating that OMB concurred with our recommendation.

In oral comments on a draft of this briefing, VA officials, including the VA/GAO Liaison, Office of Congressional and Legislative Affairs, agreed with our results. VA also provided technical comments, which have been incorporated as appropriate.

9

GAO
Accountability * Integrity * Reliability

Background

The VA data breach coupled with recent reports of other federal data breach incidents have heightened awareness of the need for agencies to be prepared to effectively respond to a breach that poses privacy risks.

While existing laws generally do not require agencies to notify affected individuals of data breaches, such notification appears to be consistent with agencies' responsibilities under the Privacy Act of 1974 and promotes accountability for privacy protection.[3]

When data breaches occur, notification has clear benefits such as allowing the affected individuals the opportunity to take steps to protect themselves from identify theft or other misuse of their personal information.

[3] The recently enacted *Department of Veterans Affairs Information Security Enhancement Act of 2006*, Pub. L. No. 109-461, requires VA to issue interim regulations for the provision of certain services, including notification, in the event a data breach of veterans' sensitive personal information results in a determination that a reasonable risk exists for the potential misuse of the information.

GAO
Accountability * Integrity * Reliability

Background

As we noted in June 2006, public notification of data breaches presents challenges as well as benefits.[4]

Determining the specific criteria for incidents that merit notification involves these important considerations:

- Notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion.
- Sending too many notices, based on overly strict criteria, could render all such notices less effective, because consumers could become desensitized to them and fail to act when risks are truly significant.
- The costs associated with notification are not insignificant for either agencies or individuals.

[4]GAO, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information*, GAO-06-833T (Washington, D.C.: June 8, 2006).

11

Background

While care needs to be taken to avoid requiring organizations to notify the public of trivial incidents, setting criteria that are too open-ended or that rely too heavily on the discretion of the affected organization could lead to inadequate notification.

To mitigate such a risk, we suggested that a two-tiered approach could be adopted, by which agencies are required to notify an entity such as OMB of *all* data breach incidents while notifying affected individuals only of incidents where there is a risk of identity theft.

Guidance subsequently issued by OMB conforms to this approach; it requires agencies to report all incidents involving PII to the Department of Homeland Security's Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident and recommending that senior agency officials make risk-based determinations of whether to inform the affected individuals.

12

Background

In addition, OMB responded to the VA data breach incident by issuing several other guidance documents in late May and June 2006 to all federal agencies. These documents directed agencies to:

- review their practices to ensure they had adequate safeguards to prevent misuse of or unauthorized access to PII; and
- use security measures, such as data encryption for mobile computers and devices, to protect data removed from an agency location.

13

Background

In a separate action, the Identity Theft Task Force was chartered by the President in early May 2006 to strengthen efforts to protect against identity theft. The task force is composed of senior officials from major federal agencies.

In September 2006, OMB issued interim guidance on data breach notification based on recommendations made by the task force. It included these recommended practices:

- Each agency should establish a core management group to respond to the loss of personal information. In the event of a loss, that group should convene to conduct a risk analysis to determine whether the incident might pose problems related to identity theft. If such a risk exists, the agency should tailor its response to the nature and scope of the risk.

14

Background

- The core management group is to include the chief information officer, chief privacy officer, chief legal officer, a senior management official, and the agency's inspector general.
- According to the interim guidance, in tailoring its response, the group should consider:
  - procuring commercial services to monitor whether a breach results in identity theft—an option that may be useful for incidents involving data gathered on large numbers of individuals,
  - offering credit monitoring services to affected individuals—a potentially expensive option—and
  - coordinating the agency's response with law enforcement through the agency's inspector general.

15

Background

- Should agencies decide to notify affected individuals, they are encouraged by the interim guidance to incorporate the following elements into the notification process:
  - Provide the notice in a timely manner, but not based on incomplete facts or in a manner likely to make identity theft more likely to occur.
  - Have a responsible official of the agency be the official source of the notice.
  - Deliver notices primarily through first class mail to the last known mailing addresses of the affected individuals.
  - Prepare for follow-on inquiries from affected individuals with Web site postings by establishing call centers and by alerting other entities, such as credit-reporting agencies.

16

GAO
Accountability * Integrity * Reliability

Background

- Further, agencies are encouraged to include the following content in their notification letters:
  - a brief description of what happened;
  - to the extent possible, a description of the types of personal information that were involved in the data security breach (e.g., full name, Social Security number, date of birth, etc.);
  - a brief description of agency actions to investigate the breach, to mitigate losses, and to protect against any further breaches;
  - contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, Web site, and/or postal address; and
  - steps individuals should take to protect themselves from the risk of identity theft, including steps to take advantage of any credit monitoring or other service the agency intends to offer and contact information for the Federal Trade Commission Web site.

17

Background

In December 2006, the *Veterans Benefits, Health Care, and Information Technology Act of 2006* (Public Law 109-461) became law. Among other things, the law specifies circumstances under which VA is required to provide credit protection services. Specifically, the law provides that:

- In the event of a data breach, an independent assessment is to be conducted by the Inspector General or another independent entity to determine the risk that the breached information may be misused;
- VA is to provide credit protection services, if the Secretary determines that a reasonable risk of misuse exists, based on the independent assessment;
- VA is to develop regulations regarding notification, data mining, fraud alerts, data breach analysis, credit monitoring, identity theft insurance, and credit protection services;
- VA is to provide reports to Congress on data breaches, including the required independent assessments, the Secretary's determinations based on the assessments, and the services offered in response.

18

GAO
Accountability * Integrity * Reliability

Background

Like VA, many other federal agencies have experienced security breaches. According to the House Government Reform Committee, since January 2003 all 19 departments and numerous federal agencies have reported at least one loss of PII that could expose individuals to identify theft.[5]

Compromised information included individual Social Security numbers, names, addresses, dates of birth, medical information, fingerprint cards, taxpayer records, and financial information.

Agencies have taken a variety of actions to notify government officials as well as the affected individuals and the public.

Attachment 1 provides case examples of recent data breaches and the responses to them at the five federal agencies we reviewed.

[5]Committee on Government Reform, *Staff Report: Agency Data Breaches Since January 1, 2003* (Washington, D.C.; Oct. 13, 2006).

19

Data Breach Notification Lessons Learned

Based on the experience of VA and other federal agencies in responding to data breaches, the following are lessons learned regarding how and when to notify government officials, affected individuals, and the public:

- Rapid internal notification of key government officials is critical.
- Because incidents vary, a committee of key officials should make decisions regarding an agency's response.
- Mechanisms must be in place to obtain contact information for affected individuals.
- Determining whether to offer credit monitoring to affected individuals requires risk-based management decisions.
- Interaction with the public requires careful coordination and can be resource-intensive.
- Internal training and awareness are critical.
- Contractor responsibilities for data breaches should be clearly defined.

20

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Rapid internal notification

Rapid internal notification of key government officials is critical.

Internal delays prevented key VA officials, including the Secretary, from being aware of the data breach until as long as two weeks after it occurred.

- The VA employee whose computer equipment was stolen on May 3, 2006, notified VA's Deputy Assistant Secretary for Policy about the incident on the same day.
- Two days later (May 5), the Acting Assistant Secretary for Policy and Planning was notified.
- In turn, the Acting Assistant Secretary informed the VA's Chief of Staff on May 9.
- Finally, the Chief of Staff informed the Secretary on May 16—almost two weeks after the theft.
- On May 22, almost three weeks after the incident, VA publicly announced the data theft. Contractors did not begin mailing initial notification letters to affected individuals on VA's behalf until June 9—more than 1 month after the incident.

21

Data Breach Notification Lessons Learned
Rapid internal notification

Because of these delays, the department's decisions about how to respond were also delayed, and, as a result, affected individuals were denied the opportunity to take prompt steps to protect themselves against the dangers of identify theft.

In addition, the public's trust and confidence in VA may have been diminished because of the slow response.

VA has taken steps to develop a uniform response policy and standard operating procedures to improve its data breach response capabilities. As part of these procedures, VA has established key organizational responsibilities for various aspects of breach response—such as roles for information security officers, the chief privacy officer, and the chief information officer—and is in the process of identifying criteria to conduct timely and uniform risk assessments and determine appropriate levels of VA response.

22

Data Breach Notification Lessons Learned
Rapid internal notification

On July 12, 2006, OMB issued guidance[6] requiring agencies to report "all incidents involving personally identifiable information in electronic or physical form" to US-CERT within one hour of becoming aware of the occurrence. The OMB guidance requires all incidents—whether suspected or confirmed—to be reported.

[6]OMB, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, Memorandum M-06-19 (Washington, D.C.; July 12, 2006).

23

Data Breach Notification Lessons Learned
Rapid internal notification

Other agencies have taken steps to improve the timeliness of their responses and have implemented the OMB guidance. For example:

- In October 2006, the Department of Transportation issued updated procedures for implementing protection of sensitive PII. It calls for all incidents involving a possible or confirmed compromise of such information to be reported to the appropriate unit's chief information officer and computer incident response team within one hour of discovery.
- In November 2006, the Department of Health and Human Services (HHS) issued procedures requiring the chief information security officer to report PII breaches within one hour of detection to the department's PII Breach Response Team and US-CERT.

If followed, these procedures should help ensure that future data breaches are addressed promptly, maximizing the opportunity for affected individuals to effectively take precautions.

24

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Core decision-making group

Because incidents vary, a core group of senior officials should be designated to make decisions regarding an agency's response.

In the VA incident, a variety of key decisions needed to be made including:

- how to work with law enforcement to recover the stolen equipment,
- what information had been compromised and what risks the theft posed,
- how affected individuals should be notified, and
- what services should be provided to assist affected individuals.

25

Data Breach Notification Lessons Learned
Core decision-making group

Cognizant officials at VA were initially unsure about who should be involved in decision making about the incident.

Since the VA incident, the Identity Theft Task Force and OMB have recommended that agencies identify a core response group that can be convened in the event of a breach to evaluate the situation and help guide further response. Among other things, the core group should:

- consist of the chief information officer, chief privacy officer, chief legal officer, a senior management official, and the agency's inspector general; and
- ensure that the agency has brought together employees who have expertise in the basic competencies needed to respond, including information technology and legal considerations (e.g., the Privacy Act).

26

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Core decision-making group

Since the data breach, VA has established an Incident Resolution Core Team consisting of key management officials including the chief information officer, chief technology officer, privacy officer, and other senior officials from VA's offices of Information Technology, General Counsel, Cyber and Information Security, Congressional Relations, Public Affairs, and Human Resources.

Officials from each of the five agencies said that they had or were in the process of establishing core management groups to respond to the loss of personal information. For example, HHS has established a PII Breach Response Team consisting of senior officials with expertise in information technology, legal requirements, privacy, law enforcement, and information security. This group is chartered to analyze incidents, evaluate the risk of identify theft, and provide guidance for further response.

Within individual agencies, establishment of a core management group should help ensure that future data breaches are addressed consistently.

27

Data Breach Notification Lessons Learned
Obtaining contact information

Mechanisms must be in place to obtain contact information for affected individuals.

VA mailed two notifications to individuals affected by the May 2006 breach: an initial notice in June and a follow-up notice in August after the stolen equipment had been recovered.

The VA did not have contact information on hand for all affected individuals. To obtain addresses for mailing the first notification letter, VA sought assistance from the Social Security Administration (SSA) and the Internal Revenue Service (IRS). SSA agreed to verify the names and Social Security numbers of the approximately 26.5 million affected individuals against data contained in its systems and delete the names and Social Security numbers of individuals that did not match SSA's records or were identified

28

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Obtaining contact information

as deceased. SSA then forwarded the verified names and Social Security numbers to the IRS. IRS agreed to forward the first round of letters on VA's behalf to individuals verified by SSA.

According to VA officials, IRS made specific legal determinations before participating in the notification process. Disclosure of personal information associated with tax returns is protected by Internal Revenue Code provisions as well as the Privacy Act of 1974. Regarding the first letter, VA officials reported that IRS had determined that the potential compromise of personal information from the VA breach could result in an impact on tax administration and thus it was appropriate to disclose address information for the purpose of notifying affected individuals.

29

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Obtaining contact information

After the first notice was issued, the stolen equipment was recovered and, based on forensic analysis, the Federal Bureau of Investigation made a determination that the data had not been compromised. As a result, VA decided to issue a second notice informing affected individuals of the status of the data breach and services that the department was continuing to offer.

However, IRS denied VA's request for addresses for the second notification because IRS concluded that, since the data had not been compromised, there was no longer any potential impact on tax administration and thus the address information could not be disclosed a second time.

To carry out the notification, VA obtained the addresses it needed from a commercial information reseller.[7]

[7]Information resellers are companies that amass and sell data, including personal data, from many sources.

30

Data Breach Notification Lessons Learned
Obtaining contact information

Other agencies also faced challenges in identifying addresses for all individuals affected by data breaches. For example:

- Although Education identified addresses for most of the individuals affected by its data breach, it was not able to contact all of them. Specifically, Education's contractor was unable to identify addresses for 60 of the 13,756 affected individuals. Of the letters it sent to the other 13,696 affected individuals, 619 were returned as undeliverable, and the contractor then identified 560 alternative addresses from parents of survey participants, school records, or public database searches and mailed the letters again with the updated address information to those addresses. This left 119 affected individuals that the department was unable to contact through these means.

31

Data Breach Notification Lessons Learned
Obtaining contact information

- Faced with the challenge of attempting to identify all affected individuals and their addresses, Agriculture decided instead to mail notification letters to all individuals included on their Tobacco Transition Payment Program mailing list. While this approach likely resulted in contact with most affected individuals, it did not provide a guarantee that all affected individuals had been reached.
- Likewise, Navy took broad action to notify affected persons of their data breach rather than attempt to identify specific affected individuals and their addresses. Navy issued an e-mail to notify all current active and reserve Marines, published a notification in a Marine quarterly newsletter issued to retired Marines, and posted two news announcements (*Washington DateLine* on 4/4/06 and *Marine Corps Times* on 4/10/06).

32

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Obtaining contact information

To improve federal agencies' ability to obtain contact information to respond to a data breach, the Identity Theft Task Force proposed directing federal agencies to publish a "routine use" for their systems of records under the Privacy Act[8] that would allow for the disclosure of information such as addresses to assist in the response to a breach of federal data.

If the disclosure of contact information in the event of data breaches is specified as a routine use, a major obstacle would be removed from other agencies providing addresses or other contact information to affected agencies.

OMB has drafted guidance that incorporates the task force's recommendation, which it plans to issue when the task force publishes its final report.

[8]A "system of records" is defined by the Privacy Act as a group of records from which information is retrieved by personal identifier. The act requires that agencies issue public notices that define, among other things, "routine uses" of the information in these systems—uses that are compatible with the purpose for which the information was originally collected.

33

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Credit monitoring

Determining when to offer credit monitoring to affected individuals requires risk-based management decisions.

VA initially decided to provide affected individuals with credit monitoring for one year. The department estimated that this would cost about $160 million. Despite the substantial cost, VA officials believed this service was an important element in protecting the personal information of veterans and their beneficiaries.

Due to the substantial anticipated cost, VA initially requested a supplemental appropriation of $131.5 million in fiscal year 2006. However, VA subsequently decided not to offer credit monitoring services after the stolen equipment was recovered and it was determined that there was little risk of misuse.

34

Data Breach Notification Lessons Learned
Credit monitoring

In deciding when to provide credit monitoring services, other agencies we reviewed primarily considered two key factors—the cost of the service and the risk of identity theft. Because of the high anticipated cost, these agencies decided not to offer credit monitoring services or to limit the availability of such services.

- For example, after considering credit monitoring services, Transportation Inspector General officials stated that their office could not afford the estimated $500,000 per month cost.

- Contractors representing Education and HHS provided credit monitoring services only to those individuals who contacted them and specifically requested the service. The notification letters sent to the affected individuals did not mention that the service was available.

35

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Credit monitoring

Other types of monitoring have been used in place of credit monitoring. For example, commercial data breach analysis services are available to analyze whether a particular data loss can be linked to reported cases of identify theft.

According to the Identity Theft Task Force, data breach analysis can assist an agency in determining whether the particular incident is the source of identity theft, or whether reported cases of identity theft are due to other causes. VA and Transportation both used data breach analysis to help monitor whether there was evidence of identity theft as a result of their data breaches.

The result of variations in approaches to credit monitoring and data breach monitoring on the part of federal agencies is that individuals who are exposed to the risk of identity theft may receive inconsistent protection depending on the varying decisions made by the agencies that suffered the data breaches.

36

Data Breach Notification Lessons Learned
Credit monitoring

The Identity Theft Task Force has noted that agencies may wish to consider offering credit monitoring services and has advised that they consider the seriousness of the risk of identity theft in doing so.

However, the task force did not develop specific guidance for making such risk-based determinations. Such guidance would characterize the risk levels of typical categories of breach incidents and recommend the type of privacy protection services that would be most appropriate for each category.

37

Data Breach Notification Lessons Learned
Credit monitoring

OMB has directed that agencies choosing to offer credit monitoring services use blanket purchase agreements managed by GSA. However, it also has not developed guidance for agencies on making risk-based determinations on when to offer credit monitoring or when to contract for data breach monitoring.

As seen in the varying decisions that federal agencies have made in how and when to offer credit monitoring, affected individuals may not always receive a consistent level of support from the federal government when their personal information is compromised. As a result, some may be more vulnerable to the adverse effects of identity theft than others. Until guidance is available to promote consistent decision-making by federal agencies, protections offered to affected individuals are likely to remain inconsistent.

38

Data Breach Notification Lessons Learned
Interaction with the public

Interaction with the public requires careful coordination and can be resource-intensive.

VA invested substantially in facilities to help address follow-on inquiries and provide information to support affected individuals.

- With the support of the General Services Administration (GSA), VA established a call center with the capacity to handle up to 260,000 calls a day. VA reprogrammed about $25 million to pay for this center. (The volume of calls received was less than VA expected; according to a GSA official, the call center received a total of about 250,000 calls.)
- VA developed a citizen telephone response plan and assigned "response approvers" to work with call center personnel who were interacting with the public.
- VA also developed an expedited approval process for updates to information regarding the data breach to ensure that complete and consistent information was made available to the public.

39

Data Breach Notification Lessons Learned
Interaction with the public

Other agencies have taken a variety of actions to establish call centers to interact with the public. For example:

- The contractor for Education set up a call center and logged each call, e-mail, or letter received from an affected individual. Through November 28, 2006, the center had logged 235 entries.
- Transportation established a hotline for affected individuals to contact if they suspected fraud. The hotline was staffed 24 hours a day, seven days a week.
- The contractor for HHS set up several call centers. From July 27 through July 31, 2006, a total of 1,406 individuals had contacted these call centers.

40

Data Breach Notification Lessons Learned
Interaction with the public

The ID Theft Task Force addressed the use of call center support in its September 2006 recommendations, which were subsequently promulgated by OMB. Specifically, the task force recommended that agencies

- Consider implementing an announcement strategy in preparing for follow-on inquiries about an incident. Such a strategy could include public statements and Web site postings.
- Prepare for follow-on inquiries from affected individuals by establishing call centers staffed with individuals prepared to answer the most frequently asked questions and by alerting other entities such as credit reporting agencies.

41

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Internal training and awareness

Internal training and awareness are critical to timely breach response, including notification.

The slow response to the May 2006 VA incident highlighted the need for personnel to be more aware of the agency's privacy and security procedures, including incident response and reporting procedures.

Effective training and awareness of agency privacy and security practices are essential for ensuring that staff are qualified to effectively carry out agency policy. Because a prompt response is critical, agency personnel must be prepared in advance with an understanding of their roles and responsibilities in responding to a data breach.

Federal guidance requires agencies to train staff at least annually on their privacy and security responsibilities before permitting access to information and information systems.

42

Data Breach Notification Lessons Learned
Internal training and awareness

Recognizing the importance of privacy training and awareness, VA took steps to reinforce its training of staff and contractors. For example,

- On May 26, 2006, VA issued a directive to its leadership to reinforce in each VA manager, supervisor, or team leader his or her duties and responsibilities in protecting sensitive and confidential information.
- VA directed all employees and contractors to complete its annual Cyber Security Awareness Training and Privacy Awareness Training by June 30, 2006. This training was designed to make VA employees aware of their responsibilities to protect sensitive information.
- VA required all employees and contractors to sign a statement of commitment and understanding subsequent to completion of the security and privacy training to confirm their understanding of the training and their commitment to protecting sensitive and confidential VA data.

43

Data Breach Notification Lessons Learned
Internal training and awareness

- During Security Awareness Week in June 2006, managers throughout VA were tasked with reviewing information security and reinforcing privacy obligations and responsibilities with their staff.
- Privacy officers were tasked with ensuring that new employees complete the agency's privacy awareness training within 30 days. They were also tasked with identifying staff who use PII and observing their adherence to privacy protection procedures.

44

Data Breach Notification Lessons Learned
Internal training and awareness

Other agencies we reviewed have also taken steps to ensure that their staff are effectively trained and aware of their privacy procedures. For example:

- Transportation launched a course to raise awareness of the proper techniques for handling and protecting personal information. The department required all employees to take this training by August 30, 2006.
- Navy took steps to have its personnel sensitized to privacy by requiring "stand down" Privacy Act training, issuing training aids, and posting new policy guidance on the department's Web site.

In its May 2006 guidance, OMB directed agencies to remind their employees of their responsibilities in safeguarding PII as well as the rules for acquiring and using it and the penalties for violating those rules.

45

GAO
Accountability * Integrity * Reliability

Data Breach Notification Lessons Learned
Contractor responsibilities

Contractor responsibilities for data breaches should be clearly defined.

While the VA data breach did not involve contractors, the issue of contractor responsibilities has figured prominently in three other recent incidents (at Agriculture, Education, and HHS).

Under the Privacy Act, a contractor operating a system of records on behalf of a federal agency is responsible for complying with the act. However, as already discussed, existing laws (including the Privacy Act) generally do not specifically address agency or contractor responses to data breaches. Contractor obligations for taking steps such as notifying affected individuals or providing credit monitoring may be unclear unless specified in the contract.

- Notifications were issued to affected individuals for each of the three data breaches involving contractors. In two of the three incidents, the contractor issued the notification.
- Two of the three contractors established call centers and provided credit monitoring services on request.

46

Data Breach Notification Lessons Learned
Contractor responsibilities

In response to the uncertainty regarding contractor responsibilities, officials from VA and HHS suggested that the Federal Acquisition Regulation address breach response requirements.

VA is in the process of establishing a VA-wide policy that ensures contractor personnel are held to the same standards as VA employees.

HHS officials said they were in the process of developing guidance requiring contractors to adhere to the department's privacy policies and for new contracts to include requirements for contractors to follow agency privacy policies.

The Identity Theft Task Force noted that when a data security breach involves a federal contractor, the responsibility for complying with notification procedures should be established with the contractor or partner prior to entering the business relationship.

OMB has drafted guidance that incorporates the task force's recommendation, which it plans to issue when the task force publishes its final report.

47

Conclusions

VA's data breach of May 2006 and other recent federal data breaches provide valuable lessons learned for agencies about responding to such incidents. Key government officials need to be informed promptly, and a designated group of agency officials must be ready to make prompt decisions about notification, which can be challenging if address information is not readily available. Careful planning is needed to be able to interact effectively with the public, training and awareness are critical, and contractor roles and responsibilities must be defined.

To its credit, OMB responded to the VA data breach by issuing guidance and forwarding recommendations by the ID Theft Task Force that largely address these lessons. However, the issue of how to make risk-based determinations on when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, has not been addressed in guidance. Without such guidance, agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals.

Recommendation

We recommend that the Director of OMB develop guidance for federal agencies on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a federal data breach.

GAO
Accountability * Integrity * Reliability

Agency Comments

An OMB Policy Analyst in the Information Policy and Technology Branch provided an e-mail message stating that OMB concurred with our recommendation. OMB noted that while it is important that individuals receive consistent responses and levels of support from federal agencies, the same response or type of support will not be appropriate in every situation. We agree that appropriate responses must be tailored to address the circumstances of the breach and believe additional guidance from OMB can facilitate consistent agency decision making about such responses.

In oral comments on a draft of this briefing, VA officials, including the VA/GAO Liaison, Office of Congressional and Legislative Affairs, agreed with our results. VA also provided technical comments, which we have incorporated into the briefing as appropriate.

50

Attachment I

Summary of Data Breaches at Five Agencies

51

Attachment I: Summary of Data Breaches at Five Agencies

Agriculture (USDA)

Date: January 19, 2006

Summary of incident:

- A Freedom of Information Act (FOIA) contractor for the Farm Services Agency inadvertently released informational CDs that contained Social Security numbers and tax identification data on tobacco producers/contract holders under the agency's Tobacco Transition Payment Program.
- On January 27, 2006, the contractor reviewed the data files that had been released and determined that they contained PII. The contractor contacted all nine individuals who had received the data and all agreed to return the unauthorized CDs and destroy any derived or copied information.

52

Attachment I: Summary of Data Breaches at Five Agencies

Number of affected individuals: approximately 350,000

Actions taken:

- The contractor reported that it had contacted a FOIA official on January 27, 2006, to inform him of the inadvertent release of PII to nine external requesters. The contractor stated that the FOIA official instructed the contractor to continue to work to recover the data and not to notify USDA management of the data breach.
- On February 9, the contractor met with USDA's chief Freedom of Information Act officer and informed him of the data breach.
- Between February 9 and 16, 2006, USDA officials assessed the nature and magnitude of the data breach to determine how to best respond.
- On February 17, 2006, the department mailed notices to all individuals on its Tobacco Transition Payment Program mailing list.

53

Attachment I: Summary of Data Breaches at Five Agencies

Department of Defense (Navy)

Date: March 14, 2006

Summary of incident:

- The Marine Corps reported the loss of a thumb drive containing PII—names, Social Security numbers, and other information—for enlisted Marines serving on active duty from 2001 through 2005. The information was being used for a research project on retention of service personnel.
- Navy officials considered the risk from the breach to be greatly diminished since the thumb drive was lost on a government installation and the drive's data were readable only through software that was password protected and "considered in limited distribution."
- Navy reported that there has been no evidence that the information was compromised.

Number of affected individuals: 207,570

54

Attachment I: Summary of Data Breaches at Five Agencies

Actions taken:

- Navy officials contacted the three credit bureaus and they agreed to offer free fraud alert on credit files of the affected individuals for up to 24 months.
- The Marine Corps took a number of actions to notify affected individuals, including:
  - issuing an electronic notice to all current active and reserve Marines on March 24, 2006;
  - publishing notification in the April-June issue of a quarterly newsletter (*Semper Fidelis)* issued to retired Marines; and
  - publishing news announcements in the *Washington DateLine* (April 4, 2006) and *Marine Corps Times* (April 10, 2006).
- The notifications, among other things, encouraged affected individuals to visit the Federal Trade Commission's Web site for identity theft guidance, informed them of free fraud alert services, and suggested that they review their credit reports for suspicious activities.

55

Attachment I: Summary of Data Breaches at Five Agencies

Education

Date: June 19, 2006

Summary of incident: A contractor for the department's National Center for Education Statistics sent a compact disc (CD) containing PII, including names and Social Security numbers via Federal Express to department officials for file-matching to the National Student Loan Data System. The CD, which was password protected, was lost in transit.

Number of affected individuals: 13,756

Actions taken:

- On Friday, June 23, 2006, Education officials contacted the contractor because they had not yet received the CD. Both the contractor and Education contacted Fed Ex on that day. Fed Ex had a record of the CD being picked up but no further information.

56

Attachment I: Summary of Data Breaches at Five Agencies

- On Monday, June 26th, the contractor called Fed Ex to let them know that the package contained a CD and to determine whether it had been located. The contractor continued to monitor the status of the lost package.
- On July 12, 2006, the contractor filed an incident report with its Institutional Review Board (IRB). The commissioner of the department's National Center for Education Statistics was made aware of the data loss on the same day that the contractor filed the incident report with its IRB. The commissioner decided that transfer of PII should cease and that a secure server should be established for the transfer of PII. Such a secure server went into use on August 1, 2006, and the restriction on data transfer was lifted.

57

Attachment I: Summary of Data Breaches at Five Agencies

- The IRB monitored the efforts, ultimately unsuccessful, to recover the lost CD. On August 15, 2006, even though the search was not finally completed, the IRB directed the contractor to draft a notification letter. At its meeting on September 19, 2006, the IRB approved the draft letter for mailing.
- On October 2, 2006, notification letters were mailed to individuals for whom address information was available (13,696 of the 13,756 affected individuals). The notice included an attached list of recommended actions in the event the affected individual noticed any suspicious activities concerning their financial accounts.
- Of the 13,696 letters that were mailed, 619 had been returned as undeliverable by November 27, 2006. Of these, the department was able to identify 560 alternative addresses and the contractor mailed the 560 letters again.

58

Attachment I: Summary of Data Breaches at Five Agencies

Health and Human Services (HHS)

Date: June 22, 2006

Summary of incident: An HHS Centers for Medicare & Medicaid Services (CMS) contractor reported the theft of a contractor employee's laptop computer from his office. The computer contained PII including names, telephone numbers, medical record numbers, and dates of birth.

Number of affected individuals: 49,572 Medicare beneficiaries

Actions taken:

- On June 22, 2006, the CMS contractor notified regional security of the incident and filed a police report.

59

Attachment I: Summary of Data Breaches at Five Agencies

- On July 10, 2006, the contractor notified CMS of the incident.
- Between July 26 and July 31, 2006, a CMS-approved notification letter was sent to the affected individuals. The letter included the CMS contractor's Notice of Privacy Practices and also provided guidance on placing fraud alerts on credit accounts by contacting the appropriate credit agencies. The CMS contractor set up call centers.
- From July 27 through July 31, 2006, a total of 1,406 members contacted the call centers. Although not offered in the notification letter, the CMS contractor offered one-year free credit monitoring to those who made telephone inquiries. A total of 141members accepted the credit monitoring service.

60

Attachment I: Summary of Data Breaches at Five Agencies

Transportation

Date: July 27, 2006

Summary of incident: A laptop computer containing PII including names, addresses, Social Security numbers, and dates of birth on Florida drivers and others was stolen from a parked car.

Number of affected individuals: Approximately 133,000 persons: 81,160 persons issued commercial drivers licenses in Miami-Dade County; 42,800 persons in Florida with Federal Aviation Administration pilot certificates; and 9,000 persons with Florida driver's licenses.

61

Attachment I: Summary of Data Breaches at Five Agencies

Actions taken:

- On August 5, 2006, after learning that the stolen laptop contained PII, the acting Inspector General (IG) immediately ordered an investigation to recover the stolen laptop. The Office of Inspector General (OIG) also established a $10,000 reward for information leading to the recovery of the laptop and/or arrest of the perpetrator.
- On August 9, 2006, the acting IG posted open letters on the OIG Web site to the Florida governor, Florida Congressional delegation and Chairs and Ranking Members of Department of Transportation Oversight Committees and Subcommittees discussing the incident.

62

Attachment I: Summary of Data Breaches at Five Agencies

- On August 14, 2006, the OIG began mailing letters to affected individuals, notifying them of the incident and providing information on actions that they could take to prevent identify theft.
- The OIG established a hotline for affected individuals to contact if they suspected fraud. The hotline was staffed 24 hours a day, seven days a week.
- The OIG also awarded a contract to a risk management company (ID Analytics, Inc.) to provide data breach analysis services to determine whether any PII of the affected individuals was being exploited. The company is to provide the IG with quarterly reports over a two-year period.

(310778) 63

Comments from the Office of Management and Budget

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

April 23, 2007

Ms. Linda D. Koontz
Director
Information Management Issues
Government Accountability Office
441 G Street, SW
Washington, DC 20548

Dear Ms. Koontz:

Thank you for the opportunity to comment on the draft Government Accountability Office (GAO) report, "Lessons Learned about Data Breach Notification" (code 310875), addressing the privacy implications resulting from data breaches.

In this report, GAO recommends that the Office of Management and Budget (OMB) develop guidance on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a federal data breach. The report also includes a definition for the term "personally identifiable information."

OMB concurs with GAO's recommendation. Consistent responses to data breaches can be achieved through consistent application of a risk-based analysis of the relevant circumstances. Providing further guidance and a risk-based framework will enable federal agencies to determine the appropriate response which is focused on treating citizens fairly, founded on the type of information lost, and commensurate with the level of risk of identity theft.

It is important for individuals affected when their personal information, including personally identifiable information, has been compromised to receive consistent responses and levels of support from the federal agency involved in the breach; however, it is important to note the same particular response and/or type of support will not be appropriate, or even necessary, for every situation.

For example, a few of the many factors considered when deciding whether to provide services following a breach, such as credit monitoring or data breach monitoring services, include the type of information lost, cost of the service being considered, risk of identity theft for the affected individuals, and likelihood the service will reduce this risk. These and other factors differ in each situation. As such, the appropriate response must be tailored to address each particular set of circumstances.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Additionally, the report includes a definition for the term "personally identifiable information" (PII) which is the same as one included in the draft policy memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," OMB recently circulated for interagency comment. OMB notes the definition of this term will likely be revised in the final policy based on comments received. As such, OMB suggests the language of the definition for PII should be clarified in the report as tentative language.

Thank you for the opportunity to review and comment on the draft report on this important issue. Protection of personal information, both generally and our response to data breaches, is vital to ensuring the trust of the American people in the federal government.

Sincerely,

Karen Evans
Administrator
Office of E-Government and
Information Technology
Office of Management and Budget

Comments from the Department of Veterans Affairs

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

April 19, 2007

Ms. Linda D. Koontz
Director
Information Management Issues
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Koontz:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report: ***Privacy: Lessons Learned about Data Breach Notification*** (GAO-07-657) and agrees with its findings. VA also agrees with GAO's recommendations that the Director of the Office of Management and Budget develop guidance for Federal agencies on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a Federal data breach.

The Department is finalizing its new data breach regulation that implements the Veterans Benefits, Health Care, and Information Technology Act of 2006, Public Law 109-461. The new Part 75 will follow the statutory framework of 38 U.S.C. 5724. Under this authority, upon the discovery of a data breach, VA must ensure that a non-VA entity or VA's Office of Inspector General conducts an independent risk analysis to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information. If the Secretary determines, based on the findings of the risk analysis, that a reasonable risk exists for the potential misuse of sensitive personal information, the statute requires that the Secretary provide notification to the affected individuals and may provide one or more of the following: credit monitoring, fraud resolution services, and identity theft insurance.

Sincerely yours,

R. James Nicholson

GAO Contact and Staff Acknowledgments

GAO Contact

Linda D. Koontz, (202) 512-6240

Staff Acknowledgments

In addition to the individual named above, other key contributors to the report were John de Ferrari, Assistant Director; Michael A. Alexander; and Nancy Glover.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548