United States Government Accountability Office

Report to Congressional Requesters

December 2013

# INFORMATION SECURITY

# Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent

GAO-14-34

GAO Highlights

Highlights of GAO-14-34, a report to congressional requesters

December 2013

# INFORMATION SECURITY

## Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent

## Why GAO Did This Study

The term "data breach" generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information. A data breach can leave individuals vulnerable to identity theft or other fraudulent activity. Although federal agencies have taken steps to protect PII, breaches continue to occur on a regular basis. In fiscal year 2012, agencies reported 22,156 data breaches—an increase of 111 percent from incidents reported in 2009 (see figure).

GAO was asked to review issues related to PII data breaches. The report's objectives are to (1) determine the extent to which selected agencies have developed and implemented policies and procedures for responding to breaches involving PII and (2) assess the role of DHS in collecting information on breaches involving PII and providing assistance to agencies.

To do this, GAO analyzed data breach response plans and procedures at eight various-sized agencies and compared them to requirements in relevant laws and federal guidance and interviewed officials from those agencies and from DHS.

## What GAO Recommends

GAO is making 23 recommendations to OMB to update its guidance on federal agencies' response to a data breach and to specific agencies to improve their response to data breaches involving PII. In response to OMB and agency comments on a draft of the report, GAO clarified or deleted three draft recommendations but retained the rest, as discussed in the report.

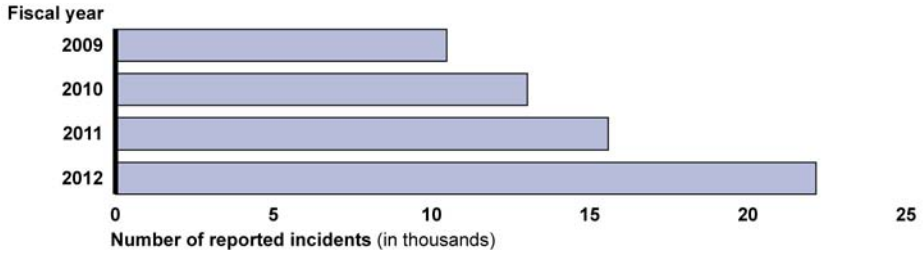
View GAO-14-34. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

## What GAO Found

The eight federal agencies GAO reviewed generally developed, but inconsistently implemented, policies and procedures for responding to a data breach involving personally identifiable information (PII) that addressed key practices specified by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology. The agencies reviewed generally addressed key management and operational practices in their policies and procedures, although three agencies had not fully addressed all key practices. For example, the Department of the Army (Army) had not specified the parameters for offering assistance to affected individuals. In addition, the implementation of key operational practices was inconsistent across the agencies. The Army, VA, and the Federal Deposit Insurance Corporation had not documented how risk levels had been determined and the Army had not offered credit monitoring consistently. Further, none of the agencies we reviewed consistently documented the evaluation of incidents and resulting lessons learned. Incomplete guidance from OMB contributed to this inconsistent implementation. As a result, these agencies may not be taking corrective actions consistently to limit the risk to individuals from PII-related data breach incidents.

According to agency officials, the Department of Homeland Security's (DHS) role of collecting information and providing assistance on PII breaches, as currently defined by federal law and policy, has provided few benefits. OMB's guidance to agencies requires them to report each PII-related breach to DHS's U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour of discovery. However, complete information from most incidents can take days or months to compile; therefore preparing a meaningful report within 1 hour can be infeasible. US-CERT officials stated they can generally do little with the information typically available within 1 hour and that receiving the information at a later time would be just as useful. Likewise, US-CERT officials said they have little use for case-by-case reports of certain kinds of data breaches, such as those involving paper-based PII, because they considered such incidents to pose very limited risk. Also, the agencies GAO reviewed have not asked for assistance in responding to PII-related incidents from US-CERT, which has expertise focusing more on cyber-related topics. As a result, these agencies may be expending resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches.

**Governmentwide Data Breach Incidents Involving PII Reported to US-CERT, 2009-2012**




Source: U.S. Computer Emergency Readiness Team (US-CERT) data.

# Contents


| | | |
|---|---|---|
| Letter | | 1 |
| | Background | 2 |
| | Agencies Generally Developed Policies and Procedures for Responding to PII-related Breaches, but Implementation Was Inconsistent | 11 |
| | The Role of DHS in Collecting PII Breach Information Within 1 Hour and Providing Assistance Offers Few Benefits to Agencies | 22 |
| | Conclusions | 26 |
| | Recommendations for Executive Action | 26 |
| | Agency Comments and Our Evaluation | 29 |
| Appendix I | Objectives, Scope, and Methodology | 34 |
| Appendix II | Comments from the Department of Defense | 38 |
| Appendix III | Comments from the Department of Health & Human Services | 41 |
| Appendix IV | Comments from the Department of Homeland Security | 44 |
| Appendix V | Comments from the Federal Deposit Insurance Corporation | 46 |
| Appendix VI | Comments from the Federal Reserve Board | 48 |
| Appendix VII | Comments from the Federal Retirement Thrift Investment Board | 50 |
| Appendix VIII | Comments from the Internal Revenue Service | 51 |

Appendix IX Comments from the Securities and Exchange Commission 56

Appendix X Comments from the Department of Veterans Affairs 58

Appendix XI GAO Contact and Staff Acknowledgments 61

Tables

Table 1: Key Management and Operational Practices to Be Included in Policies for Responding to Data Breaches Involving Personally Identifiable Information (PII) 13
Table 2: Data Breaches Involving Personally Identifiable Information (PII) Where Numbers of Affected Individuals Were Identified 18
Table 3: Number of Reported High-Risk Data Breaches Involving Personally Identifiable Information (PII) and Associated Notification Decisions 19
Table 4: Agencies Selected 34
Table 5: Number of Incidents Reviewed at Each Agency 35

Figures

Figure 1: Governmentwide Data Breach Incidents Involving Personally Identifiable Information Reported to US-CERT, 2009-2012 5
Figure 2: Operational Steps in Data Breach Response Process 16

## Abbreviations

| | |
|---|---|
| Army | Department of the Army |
| CMS | Centers for Medicare & Medicaid Services |
| Defense | Department of Defense |
| DHS | Department of Homeland Security |
| FDIC | Federal Deposit Insurance Corporation |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act of 2002 |
| FRB | Federal Reserve Board |
| FRTIB | Federal Retirement Thrift Investment Board |
| HHS | Department of Health and Human Services |
| IRS | Internal Revenue Service |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PII | personally identifiable information |
| SEC | Securities and Exchange Commission |
| US-CERT | U.S. Computer Emergency Readiness Team |
| VA | Department of Veterans Affairs |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 9, 2013

The Honorable Thomas R. Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
United States Senate

The term "data breach" generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information, including personally identifiable information (PII).[1] Having procedures in place to respond to a data breach is important in minimizing the risk of serious consequences such as identity theft[2] or other fraudulent activity that could result from such losses. Despite steps taken to protect PII at federal agencies, breaches continue to occur on a regular basis. During fiscal year 2012, federal agencies reported a record number of data breaches to the U.S. Computer Emergency Readiness Team (US-CERT).[3] Specifically, 22,156 incidents involving PII were reported—a substantial increase over the 15,584 incidents reported in fiscal year 2011.

You asked us to review issues related to agency responses to data breaches involving PII. Our objectives were to (1) determine the extent to which selected agencies have developed and implemented policies and procedures for responding to breaches involving PII and (2) assess the role of the Department of Homeland Security (DHS) in collecting

[1]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[2]Identity theft is the acquisition and use of another person's PII in a way that involves fraud or deception, typically for economic gain.

[3]US-CERT hosts the federal government's central information security incident center. When an incident occurs, agencies are required to notify US-CERT.

information on breaches involving PII and providing assistance to agencies.

We selected the following eight agencies to be included in our review: the Centers for Medicare & Medicaid Services (CMS), Departments of Army (Army) and Veterans Affairs (VA), Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), Federal Retirement Thrift Investment Board (FRTIB), Internal Revenue Service (IRS), and Securities and Exchange Commission (SEC). To select these agencies, we determined the top three large and top three independent agencies based on the number of systems containing PII they maintained. We also selected two other agencies because one experienced the largest number of data breaches involving PII in fiscal year 2011, and the other because it experienced a significant breach in 2012. We reviewed and analyzed documents from the selected agencies, including their data breach response plans and procedures, to determine whether they adhered to the requirements set forth in guidance from the Office of Management and Budget (OMB) and the National Institute for Standards and Technology (NIST) related to data breach response. In addition, we reviewed and analyzed documentation associated with a random sample of incidents from each agency's total set of reported incidents for fiscal year 2012 to determine if the selected agencies were complying with federal requirements and their respective data breach policies. Further, we reviewed relevant federal laws and OMB guidance on the involvement of DHS in the data breach response process. We also interviewed DHS officials regarding their actions in overseeing and assisting agencies in responding to a data breach involving PII. In addition, we interviewed officials from the selected agencies regarding their data breach response policies and procedures and their interactions with DHS to obtain their views on these subjects.

We conducted this performance audit from November 2012 to November 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for additional details on our objectives, scope, and methodology.

## Background

A data breach can occur under many circumstances and for many reasons. A breach can be inadvertent, such as from the loss of paper documents or a portable electronic device, or deliberate, such as from a successful cyber-based attack by a hacker, criminal, foreign nation,

terrorist, or other adversaries. Data breaches have been reported at a wide range of public and private institutions, including federal, state, and local government agencies; educational institutions; hospitals and other medical facilities; financial institutions; information resellers; and other businesses.

Protecting PII and responding to a data breach are critical because the loss or unauthorized disclosure of sensitive information can lead to serious consequences such as identity theft or other fraudulent activity and can result in substantial harm. While some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience in repairing damage to their credit records. According to the Bureau of Justice Statistics, millions of American households have reported cases of identity theft.[4]

Further, responding to a data breach can be costly. According to a judgmentally selected survey conducted by the Ponemon Institute, the average per capita cost of a data breach for U.S. companies was $188 per compromised record in fiscal year 2012.[5] On average, of the 277 companies in nine countries surveyed by Ponemon, the U.S. organizations incurred $5.4 million per breach for costs related to detecting and reporting it and for notifying affected individuals and providing credit monitoring[6] or other services.

## Data Breaches at Federal Agencies

Data breaches at federal agencies have received considerable publicity and have raised concerns about the protection of PII at those agencies. Most notably, in May 2006, VA reported that computer equipment containing PII on about 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. The following month VA sent notices to the affected individuals that explained the

[4]U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Identity Theft Reported by Households, 2005 – 2010* (Washington D.C.: November 2011).

[5]Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis*, (Traverse City, Mich.: May 2013). This study was commissioned by Symantec, a computer security software firm.

[6]Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft, thereby allowing them to take steps to minimize the harm. A credit monitoring service typically notifies individuals of changes that appear in their credit report, such as creation of a new account or new inquiries to the file.

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; however, affected individuals did not know whether their information had been misused.[7] This incident heightened awareness of the need for agencies to be prepared to effectively respond to a breach that poses security and privacy risks.

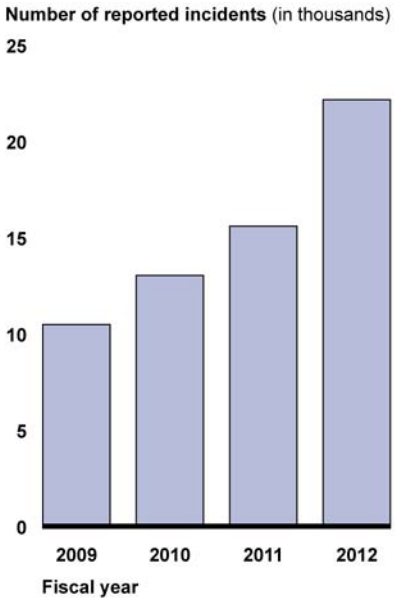
Numerous data breaches have occurred at agencies since the VA incident, including the following examples:

- In February 2009, the Federal Aviation Administration notified employees that an agency computer had been illegally accessed and that employee PII had been stolen electronically. Two of the 48 files on the breached computer server contained personal information about more than 45,000 agency employees and retirees.
- In March 2012, a laptop computer containing sensitive PII was stolen from a National Aeronautics and Space Administration employee at the Kennedy Space Center. As a result, 2,300 employees' names, Social Security numbers, dates of birth, and other personal information were exposed.
- In May 2012, the FRTIB reported a sophisticated cyber attack on the computer of a contractor that provided services to the Thrift Savings Plan. As a result of the attack, PII associated with approximately 123,000 plan participants was accessed. According to FRTIB, the information included 43,587 individuals' names, addresses, and Social Security numbers; and 79,614 individuals' Social Security numbers and other PII-related information.

According to US-CERT, the number of security incidents involving PII reported by federal agencies has increased from 10,481 incidents in fiscal year 2009 to 22,156 incidents in fiscal year 2012, an increase of 111 percent. Figure 1 shows the number of incidents at federal agencies that were reported to US-CERT from 2009 through 2012.

[7]For more information about the facts and circumstances surrounding the VA data breach incident, see GAO, *Privacy: Lessons Learned about Data Breach Notification*, GAO-07-657 (Washington, D.C.: Apr. 30, 2007).

**Figure 1: Governmentwide Data Breach Incidents Involving Personally Identifiable Information Reported to US-CERT, 2009-2012**




Source: U.S. Computer Emergency Readiness Team (US-CERT) data.

## Federal Laws and Guidance Seek to Protect PII

The Federal Information Security Management Act of 2002 (FISMA),[8] the primary law governing information security in the federal government, addresses the protection of PII in the context of securing agency information and information systems. FISMA establishes a risk-based approach to security management and sets requirements for securing information and information systems that support agency operations and assets. Under the act, agencies are required to develop procedures for detecting, reporting, and responding to security incidents, consistent with federal standards and guidelines, including mitigating risks associated with such incidents before substantial damage is done. Agencies are also required to notify and consult with other appropriate entities, such as US-CERT, law enforcement agencies, and others.

FISMA also requires the operation of a central federal information security incident center that compiles and analyzes information about incidents

[8]Pub. L. No. 107-347, Title III (Dec. 17, 2002).

that threaten information security. DHS was given the role of operating this center, which became US-CERT, by the Homeland Security Act.[9] The DHS role is further defined by OMB guidance, which requires that incidents involving PII be reported to US-CERT[10] within 1 hour of discovery. All incidents involving PII, whether suspected or confirmed, in either electronic or physical (paper) form, are required to be reported.

In addition to collecting information about data breaches, US-CERT is responsible for providing timely technical assistance to operators of agency information systems regarding security incidents, including offering guidance on detecting and handling incidents. Agency officials can request technical assistance from US-CERT in responding to a PII breach if they wish to do so.

Following the VA data breach in May 2006, additional actions were taken to strengthen controls over PII at agencies and develop more robust capabilities for responding to breaches. First, the President issued Executive Order 13402,[11] establishing the Identity Theft Task Force to make recommendations to strengthen agencies' efforts to protect against identity theft. The task force was also charged with developing a strategic plan to combat identity theft through increased awareness, better prevention and detection, and vigorous prosecution. In September 2006, the task force issued guidance for federal agencies on responding to a data breach that involved agency data, including factors to consider in determining whether to notify individuals who might be affected by the breach.[12] In April 2007, the task force released a strategic plan for combating identity theft, which included recommendations for establishing a national breach notification requirement and developing guidance

[9] Sec. 201(g)(5), Pub. L. No. 107-296 (Nov. 25, 2002).

[10] US-CERT was established by DHS to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.

[11] Executive Order 13402, *Strengthening Federal Efforts to Protect Against Identity Theft* (May 10, 2006).

[12] President's Identity Theft Task Force, *Summary of Interim Recommendations: Improving Government Handling of Sensitive Personal Data* (Washington, D.C.: Sep. 19, 2006).

regarding responding to a data breach.[13] An update was issued in September 2008.[14]

In addition, in December 2006, Congress enacted a law setting forth specific requirements for protecting PII at VA. The *Veterans Benefits, Health Care, and Information Technology Act*,[15] mandated, among other things, that VA develop procedures for detecting, immediately reporting, and responding to security incidents; notify Congress of any significant data breaches involving PII; and, if necessary, provide credit protection services to those individuals whose PII had been compromised.

Finally, OMB issued two guidance documents specifically addressing how to respond to PII-related data breaches. OMB's guidance reiterated agency responsibilities under FISMA and technical guidance developed by NIST, drawing particular attention to requirements for protecting PII.[16]

OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, issued in 2006, requires agencies to report incidents involving PII to US-CERT within 1 hour of discovering the incident.[17] It instructs agencies to report all incidents involving PII, regardless of electronic or physical form, and not to distinguish between suspected and confirmed breaches.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, was issued in 2007 in

[13]President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: Apr. 11, 2007).

[14]The President's Identity Theft Task Force Report, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: September 2008).

[15]Pub. L. No. 109-461 (Dec. 22, 2006).

[16]NIST Special Publication 800-53 (Rev. 4) provides a framework for categorizing information and information systems, and establishes minimum security requirements and baseline security controls for incident handling and reporting. (Gaithersburg, Md.: April 2013). Procedures for implementing FISMA incident-handling requirements are found in NIST Special Publication 800-61, *Computer Security Incident Handling Guide* (Gaithersburg, Md.: August 2012).

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

response to recommendations from the President's Identity Theft Task Force.[18] The memorandum requires agencies to develop and implement breach response policies and procedures within 120 days from its issuance. Key requirements include:

- adhering to FISMA requirements for detecting, reporting, and responding to security incidents;
- reporting all incidents involving PII in electronic or physical form to US-CERT within 1 hour of discovery or detection of the incident; and
- developing and implementing a breach notification policy and plan, including a policy for notifying the public. The policy is to include the following elements:
  - establish an agency response team to oversee the handling of a breach;
  - assess the likely risk of harm caused by the breach and the level of risk in order to determine whether notification to affected individuals is required;
  - determine who should be notified: affected individuals, the public, and/or other third parties affected by the breach or the notification;
  - identify who should be responsible for notifying affected individuals (generally the agency head or a senior-level individual he/she may designate in writing);
  - provide notification without unreasonable delay (with allowances for law enforcement, national security purposes, or agency needs); and
  - ensure that notification includes, among other things, a brief description of the incident, steps individuals should take to protect themselves from potential harm, if any, and what the agency is doing to investigate or protect against further breaches.

The memorandum also reiterated existing security requirements, including (1) assigning an impact level to all information and information systems, (2) implementing the minimum security requirements and controls specified in Federal Information Processing Standards 200 (FIPS)[19] and NIST Special Publication 800-53[20] respectively, (3) certifying

[18]OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007).

[19]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Washington, D.C.: March 2006).

and accrediting information systems, and (4) training employees. With regard to the first of these, OMB stressed that agencies should generally consider categorizing sensitive PII (and information systems within which such information resides) as moderate or high impact.

In addition, OMB issued three memoranda that more generally discussed protecting PII and affected individuals from potential harm. First, OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, delineated agency responsibilities to safeguard PII and to appropriately train employees in how to do so. It also required agencies to perform a review of their policies and procedures for the protection of PII, including an examination of physical security, and corrective actions to take.[21]

The second memo, *Recommendations for Identity Theft Related Data Breach Notification*,[22] listed steps that agencies should take to help affected individuals when a breach occurs. The memo stated that agencies should consider the seriousness of the risk of identity theft arising from a breach when deciding whether to offer credit monitoring services and in determining the type and length of the services.

The third memo, OMB Memorandum M-07-04, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements*, directed agencies choosing to offer credit monitoring services to use blanket purchase agreements managed by the General Services Administration.[23]

NIST has also developed related guidance on protecting PII, including:

- NIST Special Publication 800-61, *Computer Security Incident Handling Guide*,[24] which provides guidance on incident handling and reporting, including guidelines on establishing an effective incident

[20]NIST, *Information Security: Recommended Security Controls for Federal Information Systems and Organizations,* NIST Special Publication 800-53 Rev. 4, (Gaithersburg, Md.: April 2013).

[21]OMB, *Safeguarding Personally Identifiable Information*, M-06-15 (Washington, D.C.: May 22, 2006).

[22]OMB, *Recommendations for Identity Theft Related Data Breach Notification* (Washington, D.C.: Sept. 20, 2006).

[23]OMB, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements*, M-07-04 (Washington, D.C.: Dec. 22, 2006).

[24]NIST, *Computer Security Incident Handling Guide,* NIST Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

response program and detecting, analyzing, prioritizing, and handling incidents.

- NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*,[25] which includes guidelines on preventing malware[26] incidents and responding to such incidents in an effective and efficient manner.
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of PII*,[27] which provides guidance on how to develop an incident response plan to handle a breach involving PII.

## GAO Has Previously Issued Reports on Data Breaches

Since the VA data breach occurred in 2006, we have issued several reports on data breaches and the protection of PII. For example, in an April 2007 report,[28] we identified lessons learned from the VA data breach and other similar federal data breaches regarding effectively notifying government officials and affected individuals when a data breach occurs. We recommended 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. While OMB concurred with our recommendation, as of August 2013, it had not revised its PII breach guidance or issued new guidance to address when to offer credit monitoring or other services to individuals.

Also, in June 2007,[29] we reported that breaches of PII had occurred frequently across a wide range of entities and under widely varying circumstances; that most breaches had not resulted in identity theft; and

[25]NIST, *Guide to Malware Incident Prevention and Handling,* NIST Special Publication 800-83 (Gaithersburg, Md.: November 2005).

[26]Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim's system.

[27]NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NIST Special Publication 800-122 (Gaithersburg, Md.: April 2010).

[28]GAO, *Privacy: Lessons Learned about Data Breach Notification*, GAO-07-657 (Washington, D.C.: Apr. 30, 2007).

[29]GAO, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (Washington, D.C.: June 4, 2007).

that there were potential benefits, costs, and challenges associated with breach notification requirements.

In a January 2008 report,[30] we found that not all agencies had developed the range of policies and procedures to implement OMB guidance on protecting PII that is either accessed remotely or physically transported outside an agency's secure physical perimeter. OMB responded that it would continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of PII.

In June 2009,[31] we testified that the loss of PII contributes to identity theft. Specifically, we found that identity theft was a serious problem because, among other things, it might take a long time before a victim would become aware that the crime had taken place and thus cause substantial harm to the victim's credit rating. Additionally, some individuals had lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft. Even though steps had been taken at the federal, state, and local levels to prevent identity theft, vulnerabilities remained in both the public and private sectors.

## Agencies Generally Developed Policies and Procedures for Responding to PII-related Breaches, but Implementation Was Inconsistent

Overall, the agencies we reviewed have developed policies and procedures for responding to a data breach involving PII. All eight agencies had policies for the two key management practices of establishing a data breach response team and having training requirements for employees. However, only five of the agencies fully addressed each of the four key operational practices. All eight agencies had policies for reporting a suspected data breach to appropriate external entities, but the Army, FRTIB, and IRS did not fully address the other three key operational practices in their policies. Specifically, the Army did not specify parameters for offering assistance to affected individuals when appropriate in its policy or for analyzing breach response and identifying lessons learned. Further, IRS and FRTIB did not include the number of individuals affected as a factor to assess the likely risk of harm and level of impact of each incident.

[30]GAO, *Information Security: Protecting Personally Identifiable Information*, GAO-08-343 (Washington, D.C.: Jan. 25, 2008).

[31]GAO, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain*, GAO-09-759T (Washington, D.C.: June 17, 2009).

Further, a review of sample incident cases at seven of the eight agencies indicated that implementation of operational policies and procedures was not always consistent. While the agencies consistently implemented one of the key operational practices, implementation was inconsistent for the other three. Incomplete guidance from OMB contributed to this inconsistent implementation.

## Agency Policies and Procedures Generally Address OMB and NIST Guidance on Breach Response

In 2007, OMB directed agencies to develop policies that specify PII data breach reporting and handling procedures, including procedures for external breach notification.[32] In its guidance, OMB identified questions and factors each agency should consider in determining when affected individuals should be notified and the nature of such notification. Additionally, NIST has published guidelines for handling computer security incidents, including PII data breaches, that provides guidance on analyzing incident-related data and determining the appropriate response to each incident.[33] Based on our analysis of these guidance documents, the two key management and four key operational practices that agency data breach response policies should include are summarized in table 1.[34]

[32]OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (Washington, D.C.: May 22, 2007).

[33]NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,* Special Publication 800-61 Revision 2 (Gaithersburg, Md.: August 2012).

[34]The key practices listed here are those specific to the protection of PII. Information security incidents such as cyber incidents may also require technical remediation. Agencies are required to adhere to OMB and NIST guidance when responding to cyber incidents; however, we did not include cyber response activities in our review.

**Table 1: Key Management and Operational Practices to Be Included in Policies for Responding to Data Breaches Involving Personally Identifiable Information (PII)**

| Key Management Practice | Description |
|---|---|
| Establish a data breach response team | While technical remediation is usually handled by IT security staff, agencies should create a team to oversee responses to a suspected or confirmed data breach, including the program manager of the program experiencing the breach, chief information officer, chief privacy officer or senior agency official for privacy, communications office, legislative affairs office, general counsel, and the management office which includes budget and procurement functions. |
| Train employees on roles and responsibilities for breach response | Agencies should train employees on their data breach response plan and their roles and responsibilities should a breach occur. Specifically, OMB requires agencies to initially train employees on their privacy and security responsibilities before permitting access to agency information and information systems and thereafter provide at least annual refresher training to ensure employees continue to understand their responsibilities. |
| **Key Operational Practice** | |
| Prepare reports on suspected data breaches and submit them to appropriate internal and external entities | Agencies should establish procedures for promptly reporting a suspected or confirmed breach to the appropriate internal management entities and external oversight entities. For example, the breach response team should be notified about all suspected or confirmed breaches. Further, agencies must report all incidents involving PII to US-CERT within 1 hour of discovering the suspected or confirmed incident. |
| Assess the likely risk of harm and level of impact of a suspected data breach in order to determine whether notification to affected individuals is needed | In addition to any immediate remedial actions they may take, agencies should assess a suspected or confirmed breach to determine if there is a likely risk of harm and the level of impact, if applicable. OMB outlined five factors that should be considered in assessing the likely risk of harm: (1) nature of the data elements breached (2) number of individuals affected (3) likelihood the information is accessible and usable (4) likelihood the breach may lead to harm and (5) ability of the agency to mitigate the risk of harm. Once a risk level is determined, agencies should use this information to determine whether notification to affected individuals is needed and, if so, what methods should be used. OMB instructed agencies to be mindful that notification when there is little or no risk of harm might create unnecessary concern and confusion. It also stated that while the magnitude of the number of affected individuals may dictate the method chosen for providing notification, it should not be the determining factor for whether an agency should provide notification. |
| Offer assistance to affected individuals (if appropriate) | Agencies should have procedures in place to determine whether services such as credit monitoring should be offered to affected individuals to mitigate the likely risk of harm. OMB instructed agencies that, while assessing the level of risk in a given situation, they should simultaneously consider options for attenuating that risk. |
| Analyze breach response and identify lessons learned | Agencies should review and evaluate their responses to a data breach, including any remedial actions that were taken, and identify lessons learned, which should be incorporated into agency security and privacy policies and practices as necessary. NIST recommended holding a “lessons learned” meeting with all involved parties after a major incident and periodically after lesser incidents, as resources permit, to assist in handling similar incidents and improving security measures. |

Source: GAO analysis of OMB and NIST guidance.

With few exceptions, the eight selected agencies generally addressed these key practices in their policies and procedures for responding to a

data breach involving PII. Agency policies and procedures for the six key practices were as follows:

## Management Practices

- *Establish a data breach response team*: Each of the eight agencies we reviewed had developed and documented a data breach response team and designated its staff in their policies. For example, the FDIC had established a team that consisted of the FDIC Chief Information Officer/Chief Privacy Officer, the Chief Information Security Officer, the Privacy Program Manager, Information Security Managers, and representatives from the Legal Division, Office of Inspector General, Office of Legislative Affairs, Office of Communications, and authorized representatives from other divisions. The team was tasked with, among other things, providing policy, guidance, initial analysis, and direction for the potential loss of PII within the custody of the FDIC that may result in misuse or identity theft.
- *Train employees on roles and responsibilities for breach response*: Each of the eight agencies had developed and documented employee training requirements for safeguarding PII and handling incidents. For example, IRS required an annual mandatory briefing for all employees that included modules on information protection and identity theft awareness. IRS also engaged in targeted e-mail awareness campaigns focused on clarifying what PII is and how it should be protected. Similarly, FRTIB required that members of its incident response team be trained on roles and responsibilities as well as subjects such as risk and threat analysis, forensic analysis, and evidence gathering.

## Operational Practices

- *Prepare reports on suspected data breaches and submit them to appropriate entities*: All eight agencies had documented policies for preparing summary reports of suspected and confirmed data breaches. Further, all of the eight agencies we reviewed had documented policies that identified both internal and external entities that should be notified upon the discovery of an incident involving PII. For example, VA outlined reporting procedures specific to US-CERT in their incident response plan.
- *Assess the likely risk of harm and level of impact of a suspected data breach in order to determine whether notification to affected individuals is needed*: Each of the eight selected agencies had documented breach response policies that included a requirement to assess the likely risk of harm and level of impact of each incident and make a determination on whether notification to affected individuals was needed. The Army, CMS, FDIC, FRB, SEC, and VA used the five factors outlined by OMB guidance for making a risk determination. In contrast, IRS and FRTIB used only four of the five factors and did not

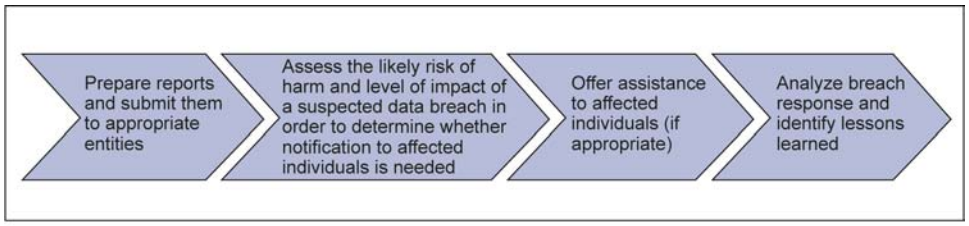
include the number of individuals affected as a factor. Without considering the number of affected individuals, IRS and FRTIB may not be appropriately determining the likely risk of harm to their agencies and level of impact of a suspected data breach.

- *Offer assistance to affected individuals (if appropriate)*: All but one of the eight agencies (the Army) had documented policies for offering services to affected individuals—specifically, credit monitoring—to help reduce the risk of identity theft. The Director for Privacy of the Defense Privacy & Civil Liberties Office stated that due to the Army's decentralized nature, the decision to offer assistance to affected individuals was the responsibility of the unit where the breach occurred. However, without documented policies for services to be offered to affected individuals, the Army runs the risk of not being able to provide consistent and reasonable protections to individuals who may have their PII compromised as a result of a breach.
- *Analyze breach response and identify lessons learned*: Seven of the eight agencies—CMS, FDIC, FRB, FRTIB, IRS, SEC, and VA—had documented policies on reviewing and evaluating incidents and responses to identify lessons learned, while one—Army—did not. For example, FRTIB's policy required its breach response team to prepare an after-action report that described lessons learned from the incident. FDIC's policy was for its response team to perform a lessons-learned assessment to consider whether modifications to incident handling procedures were needed as a final step in incident response activities, upon closure of the incident. In contrast, the Army did not include any requirements for analysis of lessons learned in their breach response policies, but officials from each agency said they have procedures that address lessons learned. For example, the Director for Privacy of the Defense Privacy & Civil Liberties Office stated that Army officials attend Department of Defense meetings where statistics and trends on departmentwide breaches are discussed and use information from these meetings to educate staff and help prevent future breaches. These reported activities are in keeping with OMB and NIST guidance. However, without having documented requirements for lessons learned from data breaches, it remains unclear whether all significant breaches will be assessed and lessons learned incorporated into the Army's practices. Thus, the Army runs the risk of not always incorporating practices and remedial actions that could decrease the likelihood of the same type of breaches recurring in the future.

## Implementation of Key Operational Practices Was Not Always Consistent

While agency policies and procedures generally adhered to OMB and NIST guidance, implementation of key operational practices was not consistent at the eight agencies we selected to review. Of these eight agencies, we evaluated seven for compliance with the four key operational practices.[35] Figure 2 summarizes the four key operational practices outlined in table 1 that agencies should take in response to a breach involving PII.

**Figure 2: Operational Steps in Data Breach Response Process**




Source: GAO analysis of OMB and NIST guidelines.

Although all seven agencies consistently implemented one of the four key operational practices, implementation was inconsistent for the other three practices. Specifically, all seven agencies prepared breach reports when suspected or confirmed incidents were identified and submitted the reports to appropriate entities. For example, incidents at IRS were documented in a form that captured information on the date the incident occurred, the incident type, the contact information of the person who reported the incident, details of the incident, and the number of affected individuals. IRS also documented the date when an incident was reported to the Department of Treasury, if required. Likewise, the Army consistently reported incidents to the Department of Defense Privacy Office, and CMS consistently reported incidents to the Department of

[35]We did not include FRTIB in our analysis of agency implementation of key operational practices because it reported experiencing only one incident involving PII in fiscal year 2012. Officials provided information on actions taken subsequent to that incident but did not provide us with documentation of the incident. The agency did not have a data breach response policy in place at the time of the incident. In a July 2012 statement to the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia, the FRTIB Executive Director stated that a breach notification plan had been put into place outlining steps that the agency would take in response to an actual or suspected data breach resulting in the loss of PII.

Health and Human Services Computer Security Incident Response Center.

However, not all seven agencies had consistently implemented the other three key operational practices. Specifically:

- *Assess the likely risk of harm and level of impact of a suspected data breach in order to determine whether notification to affected individuals is needed*: Of the seven agencies we reviewed, only IRS consistently documented both an assigned risk level and how it was determined for PII-related data breach incidents. For each of the 60 IRS incidents we reviewed, numeric scores were assigned (for the sensitivity of the data involved, the likelihood of compromise, the likelihood of harm, and the ability to mitigate the risk of harm), and a final risk determination was then recorded based on those scores.

  The Army, FDIC, and VA consistently performed a risk assessment for each of the 155 incidents we reviewed but did not document the rationale for these risk determinations. Officials from these agencies told us that they determined risk levels on a case-by-case basis and relied on staff experience and best judgment for the determination and that there was no formal requirement to document the reasons behind a risk determination. However, unless these agencies document the reasoning behind their risk determinations, they may not be able to ensure they are assessing data breaches accurately and consistently.

  CMS, FRB, and SEC generally documented neither the risk levels for the incidents we reviewed nor the rationale for their risk determinations. CMS did not document a risk level for 56 of the 58 incidents we reviewed. Officials stated that risk assessments are made in accordance with factors that are included in OMB M-07-16 and the elements present for each incident. In addition, FRB and SEC did not document risk assessments for incidents involving lost pieces of equipment containing encrypted data, such as mobile smart phones and thumb drives, which accounted for 37 out of 40 incidents at FRB and 48 out of 50 incidents at SEC. Officials from SEC stated they did not perform a separate risk assessment for each incident involving a lost agency-issued mobile device because they considered all such incidents to be of low risk, due to the implementation of encryption technology on the devices. FRB officials likewise stated that they did not consider such incidents to represent a breach of PII because the encrypted information on the devices could not be readily accessed. Since agency officials from both agencies stated they do not consider these types of incidents to be a breach, they did not perform individual

risk assessments. Nevertheless, without documenting why a risk assessment was not performed in these cases, it is difficult to determine if these agencies' policies were implemented consistently or whether all incidents involving a breach of PII were appropriately assessed.

Additionally, the seven agencies inconsistently documented the number of individuals affected by each incident. Only the Army and IRS documented the number of affected individuals for each incident we reviewed. FRB and SEC did not document the number of affected individuals for incidents involving lost pieces of equipment containing encrypted data, which was 36 and 48 incidents, respectively. Agency officials from both agencies stated they do not consider these types of incidents to be a breach, and thus they did not document the number of affected individuals for these incidents. At CMS, VA, FDIC, and FRB we found that the agencies did not always document the number of affected individuals for each case. While it may not be possible for an agency to determine the exact number of affected individuals in every case, an estimate of the number of affected individuals is important in determining the overall impact of a data breach. Until CMS, VA, FDIC, and FRB document the number of affected individuals for each incident involving PII, they run the risk of improperly assessing the likely risk of harm associated with each incident. Table 2 shows the number of data breach case files we reviewed at each agency and how many identified the number of affected individuals.

**Table 2: Data Breaches Involving Personally Identifiable Information (PII) Where Numbers of Affected Individuals Were Identified**

| | Number of incidents reviewed | | |
|---|---|---|---|
| **Agency** | **Total** | **Where affected individuals were documented** | **Where affected individuals were not documented** |
| Army | 60 | 60 | 0 |
| CMS | 58 | 31 | 27 |
| FDIC | 35 | 14 | 21 |
| FRB[a] | 40 | 1 | 39 |
| IRS | 60 | 60 | 0 |
| SEC[b] | 50 | 2 | 48 |
| VA | 60 | 0 | 60 |
| **Total** | **363** | **168** | **195** |

Source: GAO analysis of agency documentation.

Note: We did not include FRTIB in this analysis because it reported having experienced only one incident involving PII in fiscal year 2012. Officials provided information on actions taken subsequent to that incident but did not provide us with documentation of the incident.

[a]FRB only experienced four incidents that did not involve lost pieces of equipment containing encrypted data.

[b]SEC only experienced two incidents that did not involve lost pieces of equipment containing encrypted data.

The seven agencies inconsistently notified individuals affected by high-risk data breaches. While the Army and SEC notified affected individuals for all of their high-risk breaches, the other five agencies did not always notify affected individuals in cases where a high-risk determination was made. For example, for the majority of high-risk incidents at FDIC, affected individuals were not notified. Similarly, almost as many high-risk incidents at VA did not involve notification as those that did have notification. Officials from the two agencies stated that they based their determinations about notification on the type of PII that was breached rather than the level of risk assigned to the incident. However, while OMB's 2007 memorandum does not give guidance to agencies on how to use risk levels in making a determination about notification to affected individuals, it indicates that the sensitivity of the data should be an element in determining the risk of an incident. Thus it is unclear how incidents could be considered to be high risk and yet not pose a significant risk to affected individuals. Table 3 shows the number of high-risk incidents we reviewed and how many resulted in notification to the affected individuals.

**Table 3: Number of Reported High-Risk Data Breaches Involving Personally Identifiable Information (PII) and Associated Notification Decisions**

| Agency | Number of high-risk incidents | Number of incidents where affected individuals were notified | Number of incidents where affected individuals were not notified |
|---|---|---|---|
| Army | 12 | 12[a] | 0 |
| CMS[b] | | | |
| FDIC | 6 | 2 | 4 |
| FRB[c] | 0 | 0 | 0 |
| IRS | 23 | 21 | 2 |
| SEC | 1 | 1 | 0 |
| VA | 16 | 9 | 7 |
| **Total** | **58** | **45** | **13** |

Source: GAO analysis of agency documentation.

Note: We did not include FRTIB in this analysis because it reported having experienced only one incident involving PII in fiscal year 2012. Officials provided information on actions taken subsequent to that incident but did not provide us with documentation of the incident.

[a]For three of these incidents, Army records indicated an intention to notify affected individuals but did not document whether such notification was sent.

[b]CMS did not document the risk levels for 56 out of the 58 incidents we reviewed.

[c]There was one incident that did not have an assessed risk level, but individuals were notified.

FISMA directs OMB to require that agencies identify security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, such as when a breach occurs. OMB's guidance states that the risk levels should help determine when and how notification should be provided, but it does not set specific requirements for notification based on agency risk determinations. For the incidents we reviewed, the seven agencies did not make notification decisions consistently. Without better correlation between the assigned risk level and the decision to notify affected individuals, these agencies may not be consistently notifying affected individuals when they are at greatest risk of identity theft.

- *Offer assistance to affected individuals (if appropriate)*: Credit monitoring was not offered to affected individuals in a consistent manner across the seven agencies we reviewed. For example, the Army did not offer credit monitoring for any of the 60 incidents we reviewed regardless of the level of risk assigned or the number of individuals affected. Army officials told us the decision to offer credit monitoring was determined by the unit or contractor responsible for safeguarding the PII at the time the incident occurred. VA offered credit monitoring in 17 of the 60 incidents we reviewed. VA officials stated that they only offer credit monitoring when names and either Social Security numbers or dates of birth have been breached. Conversely, officials from FDIC stated that they routinely offered credit monitoring to all affected individuals. OMB guidance does not clearly state when credit monitoring should be offered to affected individuals or what factors to consider in making this determination. We previously recommended that 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. Without guidance from OMB specifying when to offer credit monitoring, the seven agencies made those determinations in varying ways. Lack of consistency in offering credit monitoring across these agencies could leave some affected individuals more exposed to identity theft than others.

- *Analyze breach response and identify lessons learned*: Lastly, none of the seven agencies we reviewed consistently documented lessons learned from PII breaches, including corrective actions to prevent similar incidents in the future or whether better security controls could help detect, analyze, and mitigate future incidents. For example, IRS and SEC did not document lessons learned for any of the 110 incidents we reviewed. IRS officials stated that they perform a quarterly and annual trend analysis that includes recommendations resulting from individual incidents. However, these recommendations were not documented. FDIC documented lessons learned for only 2 of the 35 incidents we reviewed, and FRB documented lessons learned for 3 of the 40 incidents we reviewed. FDIC officials indicated that they did not routinely perform lessons learned exercises for data breaches and did not document the results of such exercises when they were conducted because there was no requirement in the OMB guidance to do so. Three agencies—the Army, CMS, and VA—documented remedial actions, such as training and technical measures, that were to be taken to address specific incidents, but did not include an analysis of lessons learned. While OMB's 2007 guidance did not specify requirements for identifying lessons learned to help prevent future data breaches and improve incident response procedures, NIST guidance[36] states that it is important to document the major points and action items from lessons learned exercises. According to NIST, reports from such exercises could be useful in training new team members, updating incident response policies and procedures, and identifying missing steps or inaccuracies in breach response policies. Without more specific guidance on addressing and documenting lessons learned, these agencies are at risk of experiencing similar data breaches in the future and possibly suffering adverse effects that might have been prevented.

[36]NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,* Special Publication 800-61 Revision 2 (Gaithersburg, Md.: August 2012).

## The Role of DHS in Collecting PII Breach Information Within 1 Hour and Providing Assistance Offers Few Benefits to Agencies

The primary role of DHS in assisting agencies with PII-related data breaches— that of collecting information about breaches within 1 hour, as required by OMB guidance—may be difficult to fulfill and of limited value, based on the views of officials from the eight agencies we selected to review and DHS. In addition to questions about the utility of reporting incidents within 1 hour, officials also questioned the value of individually reporting paper-based incidents involving PII or incidents involving the loss of hardware containing encrypted PII. DHS uses such information primarily to compile statistical data about the prevalence of PII-related breaches, not for helping agencies to resolve or remediate such breaches. Further, the agencies we reviewed generally have not sought technical assistance from US-CERT when non-cyber PII data breaches have occurred.

### Preparing A Meaningful Incident Report Within 1 Hour Can Be Difficult

Officials at agencies and US-CERT generally agreed that the current requirement that PII-related incidents be reported within 1 hour may be difficult to meet and may not provide US-CERT with the best information. Specifically, officials at the Army, FDIC, FRB, FRTIB, and SEC indicated that it was difficult to prepare a meaningful report on a PII incident to US-CERT within the 1-hour time frame required by OMB. The officials stated that meaningful information on an incident is often not available in that time frame, and reporting an incident to US-CERT without all relevant details would likely be of limited value. While VA officials stated that most of their incidents are reported in less than an hour, they do not believe the time frame is consistent with other US-CERT reporting guidelines and that the majority of the incidents would more appropriately be reported on a weekly basis. Officials from CMS and IRS stated they did not have concerns about reporting within the given time frame but did not regard the 1-hour time frame as critically important.

FRTIB officials provided an example of a case in which 1-hour reporting was not practical. In 2012, FRTIB was notified by a contractor that the Federal Bureau of Investigation had discovered a potential breach of a computer on the contractor's system that could contain FRTIB PII. One hour after confirming that the breach contained PII, agency officials were still in the process of determining how much PII was affected and the extent of the risk. FRTIB did not have a breach response policy in place at the time of the incident. It took FRTIB approximately 5 weeks to fully understand all of the details of the breach. While they reported to US-CERT within 1 hour of confirming that the contractor breach contained FRTIB PII, it was 3 days after the contractor notified them of the suspected breach. Officials stated they would not have been able to report meaningful information if they had complied with the OMB directive

to report within an hour of when they first learned about the suspected breach.

SEC officials stated that in several instances they experienced a potential PII breach when private shipping companies lost track of boxes containing PII on paper or other media that were in transit from one SEC location to another. In such cases, the extent of PII affected or whether the package was actually lost (as opposed to an error in the shipper's tracking system) was not always clear. According to SEC officials, it can take days or weeks to fully investigate a potential loss and develop a clear assessment of its significance.

US-CERT officials also agreed that the 1-hour time frame often is not adequate for an agency to provide important information regarding an incident and does not give US-CERT a clear picture of the reported incident. Further, OMB staff said that they were unaware of the rationale for the 1-hour time frame, other than a general concern that agencies report PII incidents promptly. The staff stated that OMB previously considered revising the PII reporting guidelines but that no action had been taken. Until a more reasonable time frame is established that facilitates full reporting of meaningful information, much of the PII data breach information that US-CERT collects may be of limited value in understanding PII data breaches in government agencies.

## Agency Officials Questioned the Value of Reporting Certain Types of PII Breaches Individually

In addition to raising concerns about the reporting time frame, officials from the Army, FRB, SEC, and VA told us it was unclear to them what value was gained from individually reporting to US-CERT paper-based incidents involving PII or incidents involving the loss of hardware containing encrypted PII, because they considered such incidents to pose very limited risk. For example, in many paper-based incidents, only a few individuals are affected, thus limiting the overall risk. In cases where lost or stolen devices are protected with data encryption, officials at these agencies believe that it is very unlikely that the affected PII will be compromised. In addition, because these types of breaches generally do not involve compromises to the security of agency systems or networks, US-CERT has seldom been asked by agencies to provide assistance on remediation.

According to officials from CMS, FDIC, SEC and VA, the vast majority of incidents at these four agencies were paper incidents or involved the loss of hardware containing encrypted PII. For example, CMS officials stated that 71 percent of approximately 1,400 incidents that were reported in 2013 were paper incidents. These officials stated that most of these

cases involved PII being sent to the wrong patient or provider. In addition, VA officials stated that 76 percent of the approximately 5,000 incidents reported in fiscal year 2012 were paper incidents, which also involved PII being sent to the wrong veteran or provider. The VA officials stated that they do not see the value in reporting paper incidents individually to US-CERT as they do not have any impact on the security of their systems.

Similarly, a large number of SEC and FRB incidents involved the loss of hardware containing encrypted PII. For example, SEC reported that 98 percent of approximately 130 incidents involved the loss of hardware containing encrypted PII. SEC officials stated that they are unsure of the value of individually reporting incidents involving hardware containing encrypted PII because the risk of anyone accessing the information on the devices is very low. Likewise, the FRB's Chief Information Security Officer told us that the FRB has not reported lost hardware containing encrypted PII to US-CERT because FRB's position is that such incidents do not represent an actual loss of PII. In those cases, even though an unauthorized individual may gain access to the device, FRB's view is that it is very unlikely that the PII on it can be accessed. According to the FRB's rationale, a data breach does not occur in these cases because the data is inaccessible and thus reporting is not required. The agency's standard procedure is to issue commands to disable lost devices, rendering them inoperable and ensuring that any data they contain remains protected.

US-CERT officials agreed that their office should not be receiving all PII-related incident reports individually as they occur. For example, these officials stated that there is no reason for them to receive reports on paper-based PII breaches other than for statistical purposes in compliance with FISMA.

Current requirements to report all incidents individually can have an adverse impact by causing agencies to expend resources on activities that contribute little to protecting security and privacy. Without revisions to the reporting requirements, agencies and US-CERT will be required to continue to devote extra attention to these activities, which do not contribute to resolving or remediating data breach incidents.

## DHS Uses Reported Incident Data Primarily to Compile Statistical Information

According to the National Cybersecurity & Communications Integration Center's Chief of Compliance & Oversight and Chief of Information Management, and US-CERT's Chief of Performance Metrics, the PII-related incident data they collect are not generally used to help remediate incidents or provide technical assistance to an agency. Rather, the

information is simply compiled in accordance with the FISMA mandate of compiling and analyzing information about incidents threatening information security and reported to OMB. Given this limited use, US-CERT officials agreed that the requirement that this information be reported within 1 hour of discovery of a real or suspected breach did not add value, either for the reporting agencies or the government as a whole. US-CERT could receive the information in aggregate form at a later time, such as on a weekly or monthly basis, with no adverse impact on the quality of the statistical information, according to these officials.

Further, US-CERT's Chief of Performance Metrics confirmed that the vast majority of PII-related data breaches are not cybersecurity-related. Specifically, the official estimated that seven of every eight reported breaches do not involve attacks on or threats to government systems or networks. The Chief said that receiving information on such incidents on an individual basis is not useful to the office in pursuing its mission and that the office can take little action on the information collected about these incidents, other than to report it in aggregate form to OMB.

## Agencies Have Not Sought Technical Assistance from US-CERT Regarding PII Data Breaches

According to officials from the eight agencies we reviewed, all but one has not requested technical assistance from US-CERT when PII data breaches have occurred. According to DHS officials, US-CERT is not equipped to provide assistance in remediating paper-based incidents and has never been asked to do so.

Agency officials we spoke with agreed that the issues they encounter in dealing with PII breaches—such as what risk level to assign to an incident and whether to notify affected individuals—are not the type of issues that US-CERT can provide useful assistance to help resolve. Rather, these issues are generally best addressed by agency general counsel staff or privacy officers. These agencies' policies generally include privacy officers and general counsel staff in their incident response teams, thus providing a full complement of relevant expertise to address PII breach response.

In some cases, the DHS Privacy Office may be able to provide guidance on PII breach response. For example, the Privacy Office has developed a guide that addresses obligations of its components, employees, senior officials, and contractors to protect PII and establishes procedures they must follow upon the detection of a suspected or confirmed incident involving PII. The guidance is available to other agencies through the Privacy Office's website. In addition, Privacy Office officials stated that their office has been asked to offer guidance to other agencies on how to

best respond to incidents involving PII. However, the assistance available from the DHS Privacy Office is geared more toward developing agency response capabilities in general rather than supporting decision-making activities associated with specific incidents.

## Conclusions

The eight agencies we reviewed have taken steps to develop PII data breach response policies and procedures. Of this group, both the large and small agencies generally had policies and procedures in place that reflected the major elements of an effective data breach response program, as defined by OMB and NIST guidance. While several of these agencies had shortcomings in specific aspects of the documentation for their programs, none lacked all of the major elements. However, implementation of breach response policies and procedures was not consistent. Incomplete guidance from OMB allowed these agencies to implement data breach response policies and procedures inconsistently. Ensuring that agency data breach response programs are consistent and fully documented is an important means of ensuring that PII is fully protected.

While US-CERT plays an important role in responding to cyber incidents, including coordinating governmentwide responses and providing technical assistance to agencies, the utility of its role in responding to PII incidents is more limited, particularly when system or network issues are not involved. Given this limited role, the requirement to report all PII-related incidents within 1 hour provides little value. Likewise, immediate reporting of individual incidents involving the loss of hardware containing encrypted PII or paper-based PII to US-CERT adds little value beyond what could be achieved by periodic consolidated reporting. As a result, agencies may be making efforts to meet the reporting requirements that could be diverting attention and limited resources from other breach response activities.

## Recommendations for Executive Action

To improve the consistency and effectiveness of governmentwide data breach response programs, we recommend that the Director of OMB update its guidance on federal agencies' responses to a PII-related data breach to include:

- guidance on notifying affected individuals based on a determination of the level of risk;
- criteria for determining whether to offer assistance, such as credit monitoring to affected individuals; and

- revised reporting requirements for PII-related breaches to US-CERT, including time frames that better reflect the needs of individual agencies and the government as a whole and consolidated reporting of incidents that pose limited risk.

We are also making 22 recommendations to specific agencies to improve their response to data breaches involving PII.

- We recommend that the Secretary of Defense direct the Secretary of the Army to:
  - document procedures for offering assistance to affected individuals in the department's data breach response policy;
  - document procedures for evaluating data breach responses and identifying lessons learned;
  - require documentation of the reasoning behind risk determinations for breaches involving PII; and
  - require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.

- We recommend that the Secretary of Health and Human Services direct the Administrator for the Centers for Medicare & Medicaid Services to:
  - require documentation of the risk assessment performed for breaches involving PII, including the reasoning behind risk determinations;
  - document the number of affected individuals associated with each incident involving PII; and
  - require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.
- We recommend that the Chairman of the Federal Deposit Insurance Corporation:
  - require documentation of the reasoning behind risk determinations for breaches involving PII;
  - document the number of affected individuals associated with each incident involving PII; and
  - require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.
- We recommend that the Chairman of the Federal Reserve Board:

- require documentation of the risk assessment performed for breaches involving PII, including the reasoning behind risk determinations;
- document the number of affected individuals associated with each incident involving PII; and
- require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.

- We recommend that the Executive Director of the Federal Retirement Thrift Investment Board update procedures to include the number of individuals affected as a factor that should be considered in assessing the likely risk of harm.

- We recommend that the Commissioner of the Internal Revenue Service:
  - update procedures to include the number of individuals affected as a factor that should be considered in assessing the likely risk of harm, and
  - require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.
- We recommend that the Chairman of the Securities and Exchange Commission:
  - require documentation of the risk assessment performed for breaches involving PII, including the reasoning behind risk determinations;
  - document the number of affected individuals associated with each incident involving PII; and
  - require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.
- We recommend that the Secretary of Veterans Affairs:
  - require documentation of the reasoning behind risk determinations for breaches involving PII;
  - document the number of affected individuals associated with each incident involving PII; and
  - require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.

## Agency Comments and Our Evaluation

We sent draft copies of this report to the eight agencies covered by our review, as well as to DHS, GSA, and OMB. We received written responses from the Departments of Defense (Defense), Health & Human Services (HHS), and Homeland Security, and from FDIC, FRB, FRTIB, IRS, SEC and VA. These comments are reprinted in appendices II through X. In comments provided orally, staff from OMB's Office of Information and Regulatory Affairs stated that our draft recommendation to OMB did not sufficiently specify what supplemental guidance was needed, and we have revised our recommendation to provide greater specificity. The OMB staff also provided technical comments, which have been incorporated into the final report as appropriate. An official from GSA's IT Policy and Compliance Division indicated via e-mail that GSA had no comments.

Of the nine agencies to which we made recommendations, four (Defense, FDIC, FRTIB, and HHS) concurred with all of our recommendations. IRS agreed with one of three draft recommendations, VA agreed with one of four draft recommendations; and FRB, OMB, and SEC neither agreed nor disagreed with our recommendations. In cases where these agencies also provided technical comments, we have addressed them in the final report as appropriate. Defense, FDIC, FRB, FRTIB, HHS, and IRS also provided information regarding specific actions they have taken or plan on taking that address portions of our recommendations. Further, FDIC, FRTIB, and IRS provided estimated timelines for completion of actions that would address our recommendations.

IRS agreed with our recommendation to identify lessons learned that could be incorporated into agency security and privacy policies and practices. However, IRS did not agree with the other two draft recommendations addressed to them and provided information pertaining to those recommendations. Specifically, in response to our recommendation to update procedures to include the number of individuals affected as a factor that should be considered in assessing the likely risk of harm, IRS stated that it was following OMB guidance. IRS noted that its breach response policy contains instructions to use the number of individuals impacted to dictate the communication vehicles used for notification, and that that the number of affected individuals does not impact the potential risk to a specific individual. IRS stated that there is a higher potential risk to the agency and public for incidents involving a significant number of affected individuals and said that it has procedures for addressing incidents that affect more than 100 individuals. However, the OMB guidance cited by IRS states only that the number of individuals affected should not be the determining factor for whether an agency

should provide notification. The guidance does not say that agencies should not consider the number of individuals affected in determining the risk of harm; instead, it includes this as one of five factors that agencies should consider. IRS policy does not include the number of affected individuals as a factor in determining the likely risk of harm. We continue to believe that consideration of the number of affected individuals should be a factor in determining the likely risk of harm to the agency and level of impact of a suspected data breach, in accordance with OMB guidance and because, as IRS noted, there is a higher potential risk to the agency and public for incidents involving a significant number of affected individuals. In response to our draft recommendation to document procedures for evaluating data breach responses and identify lessons learned in the agency's data breach response policy, IRS provided additional information showing that it has such a policy in place. Accordingly, we have withdrawn this recommendation.

VA concurred in principle with our recommendation to identify lessons learned that could be incorporated into agency security and privacy policies and practices. However, VA did not concur with the other three draft recommendations addressed to the agency and provided information pertaining to those recommendations. Regarding our draft recommendation to document procedures for reporting data breaches to external entities, VA provided a recent policy update that addresses reporting to external entities such as US-CERT. Accordingly, we have withdrawn this recommendation. Regarding our recommendation to require documentation of the reasoning behind risk determinations for breaches involving PII, VA stated that the agency currently documents the reasoning behind a risk determination for each individual incident in its Privacy and Security Event Tracking System. Further, VA stated that it has developed a new tool that will be used to determine if a particular incident meets specific breach criteria that will be incorporated into a revision of VA's current breach response policies. However, our review of a sample of VA breach reports indicated that the reasoning behind risk determinations was not documented for each incident. While the new tool described by VA could serve this purpose, until it becomes part of agency policy, VA runs the risk that risk determinations may not be performed consistently. Finally, in regard to our recommendation to document the number of affected individuals associated with each incident involving PII, VA stated that it records how many individuals require notification or credit monitoring associated with an incident. Although VA's system documents information about notifications, sample breach reports we reviewed did not always include the total number of affected individuals, such as for cases in which individuals were not notified. We continue to

believe that it is important to document the number of affected individuals for all incidents involving PII.

FRB neither agreed nor disagreed with our three recommendations. In response to all of our recommendations, FRB stated that the board documents incidents in which a potential breach does not involve lost encrypted equipment, distinguishing such incidents from losses of encrypted equipment, which the agency generally did not consider to be potential breaches of PII. However, FRB stated that it will review its practices to ensure that it more comprehensively documents potential PII breaches, including, as appropriate, incidents involving lost encrypted equipment.

SEC neither agreed nor disagreed with our three recommendations but provided information concerning each of them. Specifically, in response to our recommendation to require documentation of risk assessments, SEC stated that the Commission considers incidents involving encrypted equipment to be covered by a previously reported incident where the SEC assessed a low level of risk and set forth its rationale for this risk determination. Further, SEC stated that such devices can be remotely erased in the event of loss. According to SEC, it believes that preparing a separate risk assessment for each incident involving encrypted, remotely managed devices does not provide meaningful value to the data breach process. We believe it is important to document risk determinations for every incident, including the reasons why a risk assessment was not performed in cases such as the ones cited by the SEC, to ensure that all incidents involving a breach of PII are appropriately assessed. Ensuring that all incidents are properly documented would not require extra, unnecessary effort (because a reference to a previous determination, if appropriate, could be used). However it would help ensure that the agency has not overlooked incidents that may have greater risks. In response to our recommendation to document the number of affected individuals associated with each incident involving PII, SEC stated that for incidents involving lost encrypted devices, the risk of compromise is low to non-existent and as a result, the number of potentially affected individuals is immediately mitigated to a negligible number. While OMB guidance states that the use of encryption ensures that the risk of compromise is low, it does not conclude that “the number of potentially affected individuals is immediately mitigated to a negligible number.” We continue to believe that it is important to document the number of affected individuals for each incident involving PII so that the likely risk of harm is properly assessed for each incident and so that an accounting of the total number of affected individuals for all data breach incidents is possible.

Lastly, in response to our recommendation to require an evaluation of the agency's response to data breaches involving PII to identify lessons learned, SEC stated that as a part of its privacy incident reporting process, it assesses mitigation measures and identifies security controls that could help detect, analyze, and mitigate future incidents and makes recommendations when applicable. However, the SEC's periodic recommendations for new or revised security controls does not specifically include a review of past incidents to determine whether proposed changes to security controls address vulnerabilities identified in past incidents. We continue to believe that it is important to document these lessons learned from prior incidents involving PII to help ensure the agency does not overlook additional actions that could be taken to prevent future incidents.

DHS provided information regarding actions it plans on taking to help address our recommendations to OMB on revising its incident reporting requirements. Specifically, DHS stated it has interacted with OMB regarding requirements specific to these recommendations and is preparing new incident reporting guidance for agencies to be presented to members of the Federal Chief Information Officers Council Security Program Management Subcommittee. We also received technical comments from DHS, which have been incorporated into the final report as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Departments of Defense, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs, as well as the Federal Deposit Insurance Corporation, Federal Reserve Board, Federal Retirement Thrift Investment Board, General Services Administration, Office of Management and Budget, and Securities and Exchange Commission. In addition, the report is available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public

Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Gregory C. Wilshusen
Director, Information Security Issues

# Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the extent to which selected agencies have developed and implemented data breach response policies and procedures for breaches involving PII and (2) assess the role of DHS in collecting information on breaches involving PII and providing assistance to agencies.

We selected four large agencies and four independent agencies to be included in our review. To select these agencies, we first determined the top three agencies in each category that had the largest number of systems containing PII they maintained, according to fiscal year 2011 agency reports submitted in compliance with requirements of FISMA. We also selected VA as one of the large agencies for review because it experienced the largest number of data breaches involving PII in fiscal year 2011, and we chose FRTIB as an additional independent agency because it experienced a significant breach in 2012. For three of the large agencies, we limited our review to the component within the agency that had the greatest number of systems containing PII. Table 4 lists the agencies we selected.

**Table 4: Agencies Selected**

| Agency | Category |
|---|---|
| Department of the Army | Large |
| Centers for Medicare & Medicaid Services | Large |
| Internal Revenue Service | Large |
| Department of Veterans Affairs | Large |
| Federal Deposit Insurance Corporation | Independent |
| Federal Reserve Board | Independent |
| Federal Retirement Thrift Investment Board | Independent |
| Securities and Exchange Commission | Independent |

Source: GAO.

To address our first objective, we reviewed OMB memorandum M-07-16 and NIST Special Publication 800-61 Revision 2 to determine the key elements that should be present in data breach response programs at federal agencies. We then reviewed and analyzed documents from the selected agencies, including data breach response plans and procedures, to determine whether they adhered to the requirements set forth in OMB and NIST guidance. In addition, we interviewed agency officials from the selected agencies regarding their data breach response policies and procedures.

To address implementation of data breach response policies and procedures for breaches involving PII, we reviewed and analyzed documentation associated with a random sample of incidents from all but one agency's total set of reported incidents for fiscal year 2012 to determine if the agencies were complying with federal requirements and their respective data breach policies. In the analysis, we determined whether the agencies had prepared reports on suspected or confirmed breaches and submitted them to the appropriate internal and external entities, assessed the likely risk of harm and level of impact of a suspected data breach in order to determine whether notification to affected individuals was needed, offered assistance to affected individuals, and analyzed breach response and identified lessons learned. We did not include FRTIB in this analysis because it reported having experienced only one incident involving PII in fiscal year 2012. While information was provided on actions taken subsequent to that incident, officials did not provide us with documentation resulting from that incident. We selected a simple random sample of incidents within each of the remaining seven agencies. In order to support estimation for the population of incidents across the seven agencies, the seven simple random samples were grouped and treated as a stratified random sample for purposes of producing estimates. Table 5 lists the number of incidents we examined at each agency.

**Table 5: Number of Incidents Reviewed at Each Agency**

| Agency | Number of reported incidents in FY2012 | Number selected for review | Margin of error |
|---|---|---|---|
| Department of the Army | 399 | 60 | +/- 12.5 |
| Centers for Medicare & Medicaid Services | 4172 | 58[a] | +/- 13.1 |
| Internal Revenue Service | 3696 | 60 | +/-13.0 |
| Department of Veterans Affairs | 6627 | 60 | +/- 13.1 |
| Federal Deposit Insurance Corporation | 51 | 35 | +/- 12.2 |
| Federal Reserve Board | 59 | 40 | +/- 11.0 |
| Securities and Exchange Commission | 136 | 50 | +/- 11.8 |
| **Total** | **15,140** | **363** | |

Source: GAO.

Note: We did not include FRTIB in this analysis because it reported having experienced only one incident involving PII in fiscal year 2012 and officials did not provide us with documentation resulting from that incident. Officials provided information only on the actions that were taken in response to that incident.

[a]CMS stated that two of the incidents we selected for review were duplicate records and did not provide documentation for those incidents.

Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval. This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn. All agency-specific percentage estimates from the file review have margins of error at the 95 percent confidence level that are no greater than the amounts shown in table 4. For population estimates derived from combining the seven samples, percentage estimates have a margin of error at the 95 percent level of confidence that is no greater than plus or minus 7.2 percentage points unless otherwise noted.

To determine the reliability and accuracy of the data, we obtained and analyzed answers to 20 data reliability questions from each agency that addressed the internal controls of the system used to collect the data. Specifically, we asked questions regarding systems that had current data, procedures in place to consistently and accurately capture data, controls that check for errors in data, reviews of the data, system failures, and the overall opinion of the agency on the quality of its data. In addition, we performed electronic testing on the data to check for missing values and out-of-range incident dates. We believe the data used to draw our sample are sufficiently reliable for the purpose of this report.

To address the second objective, we reviewed relevant federal laws and guidance on the involvement of DHS in the data breach response process. We also performed an analysis to determine whether the sample cases we reviewed reported the incidents to US-CERT within the required 1-hour time frame. In addition, we interviewed DHS officials regarding their actions in overseeing and assisting agencies in responding to a data breach involving PII. Further, we interviewed agency officials from the selected agencies regarding their interactions with DHS and their views on this interaction.

We conducted this performance audit from November 2012 to November 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Comments from the Department of Defense

ADMINISTRATION AND MANAGEMENT

**OFFICE OF THE SECRETARY OF DEFENSE**
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

NOV 25 2013

Dear Mr. Wilshusen:

On behalf of the Secretary of Defense, this letter and attachment is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-14-34, "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent," dated October 23, 2013 (GAO Code 311098). DoD concurs with the four recommendations addressed to the Secretary of Defense.

DoD administers a comprehensive privacy program, through the Defense Privacy Civil Liberties Office (DPCLO), based on centrally established policy requirements and decentralized implementation throughout the DoD Components. To that end, DPCLO issued policy in compliance with the Office of Management and Budget (OMB) Memorandum M-07-16 dated May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." A corresponding DoD memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," was issued on June 5, 2009, to implement policy changes to reflect the requirements of that OMB memorandum. An additional DoD memorandum was issued on August 2, 2012, "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations" establishing best judgment criteria to help guide components toward optimal decision-making regarding PII breach risk and notification determinations.

Neither DoD memorandum fully addresses the recommendations made to the Secretary of Defense in the GAO report. To satisfy these recommendations, DPCLO intends to consolidate these two DoD memorandums and revise requirements in order to establish appropriate policies and procedures to address the GAO's recommendations. To ensure DoD-wide application of the new guidance, the combined issuance will be addressed to and made applicable to all DoD Components.

If you have any questions, please contact my primary action officer, Mr. Samuel P. Jenkins at 703-571-0070 or e-mail samuel.p.jenkins.civ@mail.mil.

Sincerely,

Michael Rhodes
Senior Agency Official for Privacy

Attachment:
As stated

**GAO DRAFT REPORT DATED OCTOBER 23, 2013**
**GAO-14-34 (GAO CODE 311098)**

"Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consist"

**DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION**

**RECOMMENDATION 1**: The GAO recommends that the Secretary of Defense direct the Secretary of the Army to document procedures for offering assistance to affected individuals in the Department's data breach response policy.

**DoD RESPONSE**: (Concur) DoD administers a comprehensive privacy program, through the Defense Privacy Civil Liberties Office (DPCLO), based on centrally established policy requirements and decentralized implementation throughout the DoD Components. To that end, DPCLO issued policy in compliance with the Office of Management and Budget (OMB) Memorandum M-07-16 dated May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." A corresponding DoD memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," was issued on June 5, 2009, to implement policy changes to reflect the requirements of that OMB memorandum. An additional DoD memorandum was issued on August 2, 2012, "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations" establishing best judgment criteria to help guide components toward optimal decision-making regarding PII breach risk and notification determinations.

Neither DoD memorandum fully addresses the recommendations made to the Secretary of Defense in the GAO report. To satisfy these recommendations, DPCLO intends to consolidate these two DoD memorandums and revise requirements in order to establish appropriate policies and procedures to address the GAO's recommendations. To ensure DoD-wide application of the new guidance, the combined issuance will be addressed to and made applicable to all DoD Components.

**RECOMMENDATION 2**: The GAO recommends that the Secretary of Defense direct the Secretary of the Army to document procedures for evaluating data breach responses and identifying lessons learned.

**DoD RESPONSE**: (Concur) See response to Recommendation 1 above.

**RECOMMENDATION 3:** The GAO recommends that the Secretary of Defense direct the Secretary of the Army to require documentation of the reasoning behind risk determinations for breaches involving PII.

**DoD RESPONSE**: (Concur) See response to Recommendation 1 above.

2

**RECOMMENDATION 4:** The GAO recommends that the Secretary of Defense direct the Secretary of the Army to require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.

**DoD RESPONSE**: (Concur) See response to Recommendation 1 above.

# Appendix III: Comments from the Department of Health & Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

NOV 25 2013

Gregory C. Wilshusen, Director
Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) draft report entitled, "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent" (GAO 14-34).

The Department appreciates the opportunity to review and comment on this report prior to publication.

Sincerely,

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "AGENCY RESPONSES TO BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION (PII) NEED TO BE MORE CONSISTENT" (GAO-14-34)**

The Department appreciates the opportunity to review and comment on this draft report.

The draft report contains three recommendations for the Secretary of HHS to direct to the Administrator of the Centers for Medicare & Medicaid Services (CMS). HHS responds to the recommendations below:

**GAO Recommendation:**
Require documentation of the risk assessments performed for breaches involving personally identifiable information (PII), including the reasoning behind risk determinations.

**HHS Response:**
HHS concurs with this recommendation. In 2013, CMS engaged in process improvement by connecting its incident reporting system to the HHS system. This change has resulted in complete information being reported on each CMS incident, including the level of risk assessment, maintained in one system. In addition, each incident reporting form is attached in the system's database, thereby ensuring documentation includes all updates and mitigation activities in support of the reasoning behind the risk determination. CMS continues to work closely with HHS to improve responses to data breaches.

**GAO Recommendation:**
Document the number of affected individuals associated with each incident involving PII.

**HHS Response:**
HHS concurs and has already implemented GAO's recommendation. In 2013, CMS made changes to improve its incident response processes which have resulted in the number of affected individuals associated with a PII incident being reported and documented. This information is now being consistently collected on each incident reporting form and entered into CMS' incident reporting system. Prior to this process improvement, a manual process was used to track this information. The CMS database now contains complete documentation on CMS incidents, including the number of affected individuals associated with a PII incident.

**GAO Recommendation:**
Require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.

**HHS Response:**
HHS concurs with this recommendation. In 2013, agency privacy and security staff collaborated in lessons learned on incidents with high visibility. This process is documented in the agency's Incident Handling Procedure as part of the follow-up phase of incident response. In addition, during CMS' annual privacy and security awareness week, agency staff was made aware of the most common issues on incidents reported throughout the year. Information was distributed by flyers, providing web links, and during one-on-one discussions with agency staff. The objective of privacy and security awareness week activities is providing outreach and education on these

1

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "AGENCY RESPONSES TO BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION (PII) NEED TO BE MORE CONSISTENT" (GAO-14-34)**

issues to minimize the most common breaches and security incidents that occur at the agency. CMS will continue to refine its processes to identify lessons learned and incorporate information in privacy and security policies and practices, as appropriate.

2

# Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 22, 2013

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-14-34, "INFORMATION SECURITY: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's acknowledgment of DHS's U. S. Computer Emergency Readiness Team (US-CERT), within the National Protection and Programs Directorate's Office of Cybersecurity and Communications and its important role when responding to cyber incidents. This includes, among other things, coordinating government-wide responses and providing technical assistance to Federal agencies.

GAO also noted that the utility of US-CERT's role in responding to Personally Identifiable Information (PII) incidents is limited, particularly when system or network issues are not involved. In addition, GAO concluded that given this limited role, the requirement to report PII-related incidents within the one hour timeframe provides little value. As a result, agencies may be making efforts to meet the reporting requirements that could be diverting attention and limited resources from other breach response activities.

The draft report contained no recommendations intended specifically for DHS; however, GAO recommended that the Director of the Office of Management and Budget (OMB) update its guidance on Federal agencies' responses to PII-related data breaches including:

- Criteria for determining when to notify affected individuals and whether to offer assistance, such as credit monitoring; and
- Revised reporting requirements for PII-related breaches to US-CERT, including time frames that better reflect the needs of individual agencies and the government as a whole and consolidated reporting of incidents that pose limited risk.

During the coming months, US-CERT will meet regularly with OMB to discuss planning to address and closeout these actions. Accordingly, US-CERT has worked closely with the

National Institute of Standards and Technology (NIST) and has already begun engaging with OMB for the purposes of gathering requirements specific to these actions and will support OMB in ongoing efforts to achieve the goals as outlined below.

Specifically, DHS is preparing new incident reporting guidance for the Departments and Agencies in alignment with the "DHS Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for Homeland Security Enterprise" (November 2011) and NIST Special Publication "Computer Security Incident Handling Guide" (SP 800-61 Revision 2). This new guidance will be presented to members of the Federal Chief Information Officers Council Security Program Management Subcommittee in December 2013. DHS also anticipates circulating the guidelines for comment and having a draft with comments by January 31, 2014, in addition to having a draft FY 2014 Federal Information Security Memoranda for OMB's consideration by March 31, 2014.

Ultimately, DHS's goal is to begin phasing in any new incident reporting protocol issued by OMB and to provide all Departments and Agencies with a sufficient grace period to ensure their incident reporting systems and procedures can be transitioned smoothly to the new system by December 31, 2014.

Again, thank you for the opportunity to review and provide comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

# Appendix V: Comments from the Federal Deposit Insurance Corporation

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Office of the Chief Information Officer

November 22, 2013

Mr. John de Ferrari
Assistant Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. de Ferrari:

Thank you for the opportunity to comment on the U.S. Government Accountability Office's (GAO) draft report titled, *Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO-14-34. The report presents the GAO's analysis of eight agencies' data breach response plans and procedures as compared to requirements in relevant laws and Federal guidance.

We are pleased that the GAO's draft report, in general, recognized that the agencies, including the FDIC, had developed policies and procedures for responding to data breaches involving personally identifiable information (PII), which included two key management practices relating to the establishment of a data breach response team and the development and documentation of training requirements for employees.

The GAO's draft report generally concluded, however, that more work is needed by the agencies to address the key operational practices identified in the draft report and to ensure greater consistency when implementing agency breach policies and procedures. Toward that end, the GAO provided three recommendations specific to the FDIC intended to strengthen our breach response process. The FDIC accepts all three recommendations and is taking specific action to be completed by June 30, 2014 to address each recommendation as briefly described below:

**GAO Audit Recommendation #1.** *Require documentation of the reasoning behind risk determinations for breaches involving PII.*

**FDIC Response**: The FDIC concurs with the recommendation. Based on a further review of the six high-risk incidents noted in the draft report (Table 3, page 22), we are pleased to report that the FDIC appropriately documented its risk determinations and notifications decisions in all instances. However, we recognize that the information was not always readily or easily accessible. The FDIC is taking steps to review and strengthen the documentation process for breaches involving PII, including the supporting case file information, to facilitate greater understanding of the reasoning behind risk determinations and the timely offer of credit monitoring services to affected individuals, when applicable.

**GAO Audit Recommendation #2.** *Document the number of affected individuals associated with each incident involving PII.*

**FDIC Response**: The FDIC concurs with the recommendation. Based on a further review of the thirty-five (35) incidents identified in the draft report (Table 2, page 21), we are pleased to report that the FDIC appropriately documented the number of individuals affected in 20 out of the 35 incidents, including two that were the responsibility of other public entities. We also determined that, for 14 out of the 15 remaining incidents, the PII was encrypted and thereby not considered to be at risk of breach or the PII was discovered in a network file share where the risk of breach was considered to be low. Therefore, there was no benefit in documenting the number of individuals. We are re-evaluating our current process related to identifying and documenting the number of potentially affected individuals with the intent of improving the process, as appropriate, to ensure that it aligns with Federal requirements and industry best practices. Our re-evaluation will take into consideration our response efforts related to incidents where data is fully encrypted or discovered in internal network file shares where access controls have been improperly configured.

**GAO Recommendation #3**: *Require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.*

**FDIC Response**: The FDIC concurs with the recommendation. While not required by law or regulation, we are pleased to report that, as a best practice, the FDIC does require the conduct of lessons learned for complex or unique breaches. We are in the process of reviewing and revising our data breach guidance to make more explicit the need to conduct lessons learned for all applicable breaches.

The FDIC takes seriously its responsibility to protect the privacy of individuals and to safeguard PII. We know that preventing the loss of PII is essential to maintaining the trust of the public. We thank the GAO staff for their in-depth audit and remain committed to continually improving our risk-based breach response process.

If you have any questions or concerns, please don't hesitate to contact me at (703) 254-0190.

Sincerely,

Martin Henning
Acting Chief Information Officer and
Chief Privacy Officer

2

# Appendix VI: Comments from the Federal Reserve Board

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

DIVISION OF
INFORMATION TECHNOLOGY

Mr. Gregory C. Wilshusen, Director
Information Security Issues
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on your draft report, GAO 14-34, about Agency responses to data breaches involving Personally Identifiable Information ("PII").

The draft report confirms that the Federal Reserve Board ("Board") follows the Key Management and Operational Practices for data breaches involving PII as directed by the OMB. These steps include: establishing a data response team; training employees in breach response procedures; reporting on suspected data breaches; assessing the likely harm and level of impact of the suspected breach; offering assistance to affected individuals (if appropriate); and analyzing the breach response and lessons learned. As the report notes, the Federal Reserve Board experienced no high risk data breach incidents involving PII for the period reviewed, and the vast majority of incidents the GAO reviewed involved equipment protected through encryption, including equipment that could be erased remotely.

The draft report includes 24 recommendations to the agencies the GAO reviewed, three of which are directed to the Board. The three recommendations relate to more comprehensively documenting incidents of potential PII breaches in the areas of risk assessment, numbers of individuals affected, and evaluations of Board responses including lessons learned. The Board already documents incidents in which a potential breach does not involve lost encrypted equipment; distinguishing such incidents from losses of encrypted equipment which, arguably, are not potential breaches of PII. In response to the report, the Board will review its practices to ensure that, as GAO recommends, the Board more comprehensively documents potential PII breaches, including, as appropriate, for incidents involving lost encrypted equipment.

www.federalreserve.gov

2

We appreciate the GAO's work in this area and for the opportunity to review the draft report.

Sincerely,

Sharon Mowry,
Director,
Information Technology Division

# Appendix VII: Comments from the Federal Retirement Thrift Investment Board

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77K Street, NE Washington, DC 20002

November 22, 2013

Mr. Gregory C. Wilshusen
Director, Information Technology
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

This letter conveys the Federal Retirement Thrift Investment Board's (FRTIB) response to the recommendation contained in the Government Accountability Office's report entitled "Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent." The information developed as a result of this report will be useful to the continued improvement of the TSP.

The Government Accountability Office (GAO) report directs one recommendation to the FRTIB. Our response to this recommendation is discussed below.

Recommendation No. 1: *We recommend that the Executive Director of the Federal Retirement Thrift Investment Board update procedures to include the number of individuals affected as a factor that should be considered in assessing the likely risk of harm.*

**Response:** We concur with this recommendation. The Agency will update its Data Breach plan to include the number of individuals affected as a factor that should be considered in assessing the likely risk of harm. We expect to complete this action by December 15, 2013.

Sincerely,

Gregory T. Long
Executive Director

# Appendix VIII: Comments from the Internal Revenue Service

DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

November 25, 2013

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the Government Accountability Office's report titled *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent (GAO-14-34)*. The IRS takes the issue of data breaches very seriously, and we are committed to ensuring that the IRS follows all applicable guidance for federal agencies to respond to data breaches involving Personally Identifiable Information (PII).

The IRS maintains a well-documented data breach analysis process. We continually review and enhance our policies and procedures to ensure taxpayer information is protected and the appropriate actions are taken when a breach occurs. We appreciate your recognition of our extensive data breach procedures that include a thorough documentation of the incident details and determination of the risk of harm resulting from the breach.

While the report does recognize many of our existing procedures, it does not reflect IRS's compliance with requirements of Office of Management and Budget Memorandum 07-16 (OMB M 07-16) *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. The IRS already considers the number of individuals affected by the breach as a factor when assessing the likely risk of harm. The IRS also documents procedures for evaluating data breach responses and identifying lessons learned by determining the root cause of the incident and identifying preventive measures.

We agree with the GAO's recommendation to evaluate our response to data breaches involving PII to identify lessons learned that could be incorporated into agency security

2

and privacy policies and practices. Our detailed responses to the recommendations are enclosed.

If you have any questions, please contact me at (202) 622-4255, or a member of your staff may contact Rebecca Chiaramida, Director, Office of Privacy, Governmental Liaison and Disclosure, at (202) 317-6449.

Sincerely,

Peggy Sherry
Deputy Commissioner for Operations Support

Enclosure

**Enclosure**

**Government Accountability Office's (GAO) Draft Report: Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent (GAO-14-34)**

**RECOMMENDATION 1:**

Update procedures to include the number of individuals affected as a factor that should be considered in assessing the likely risk of harm.

**CORRECTIVE ACTION:**

Our current procedures follow the guidance outlined in OMB Memorandum M-07-16, which states: "[t]he magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification."

Following this guidance, IRS procedures contain the following instructions in Section 3 of the IRS Breach Response Analysis: "OMB suggests a fifth factor: the number of individuals impacted. This element should not be used to determine if notification should be provided, but may dictate the communication vehicles used for notification."

The number of individuals does not impact the potential risk to a specific individual when their PII is disclosed. The risk to a single individual whose information is disclosed is as high as the risk to multiple individuals whose information is disclosed. While the number of individuals is not one of the four factors used to determine the potential risk to a specific individual, the IRS recognizes the higher potential risk to the agency and public for incidents involving a significant number of affected individuals.

As GAO acknowledged, the IRS is one of only two agencies that document the number of affected individuals for every incident. If the number of potentially impacted individuals is at least 100, IRS has specific procedures detailed in the Incident Management Operations Guide, Section 1.2, Escalation Process for High Impact Incidents, to elevate the incident to Privacy Government Liaison and Disclosure (PGLD) management and other impacted offices. The escalation of incidents with a large number of affected individuals allows for the expedited development of preventive actions and gives the appropriate organizations a head start to work the issue.

**IMPLEMENTATION DATE:**
N/A

**RESPONSIBLE OFFICIAL:**
Director, Privacy, Governmental Liaison & Disclosure

**CORRECTIVE ACTION MONITORING PLAN:** N/A

2

**RECOMMENDATION 2:**

Document procedures for evaluating data breach responses and identifying lessons learned in the agency's data breach response policy.

**CORRECTIVE ACTION:**

Our existing procedures identify lessons learned by determining the underlying cause and identifying the preventive measures. Under the existing written procedures of the Incident Management Operations Guide, Section 1.2, Escalation Process for High Impact Incidents, Incident Management (IM) staff complete a template for high profile incidents (high volume of affected individuals, unusual circumstances, and other high profile situations) that is shared with PGLD management and other impacted offices.

As part of the analysis for these types of incidents, the IM analyst works with the reporting office to determine the underlying cause and to identify the preventive measures that will help reduce the probability of the same type of incident occurring in the future. The template (Incident Management Operations Guide Exhibit 8 – Incident Report Template) contains fields where the cause of the error and the preventive measures planned for the future are documented.

**IMPLEMENTATION DATE:**
N/A

**RESPONSIBLE OFFICIAL:**
Director, Privacy, Governmental Liaison & Disclosure

**CORRECTIVE ACTION MONITORING PLAN:**
N/A

**RECOMMENDATION 3:**

Require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.

**CORRECTIVE ACTION:**

We agree with this recommendation and will update the procedures in the IRS Breach Response Analysis to include our existing process for identifying lessons learned that can be incorporated into our security and privacy policies and practices. The IRS currently conducts an analysis of the agency's response to data breaches through the trend analysis report and Business PII Risk Assessment (BPRA) processes, but these procedures are not currently documented within the IRS Breach Response Analysis.

3

As stated in the GAO report, IRS completes an annual Trend Analysis Report that contains a detailed analysis of the incidents reported for the fiscal year. The Trend Analysis Report is shared with the PII Working Group and the Data Loss Prevention Working Group. Both groups are comprised of functional representatives and provide forums to discuss privacy related concerns with privacy staff, business unit front line management, and other team members. Through these partnerships, procedural and process improvements are identified and shared throughout the agency, thereby helping reduce the number of incidents and associated potential risk of harm to taxpayers.

The report is also shared with the Privacy Compliance office in PGLD to determine if there are any processes for which a BPRA can be performed and with the Think Data Protection program to use as a basis for identifying additional areas of focus for employee communication. The data was recently used by Privacy Compliance to identify the need for a BPRA on faxing procedures. The BPRA reports identify vulnerabilities and make recommendations for changes to improve the agency's security and privacy policies and practices. Documentation regarding the trend analysis and BPRA processes will be included in the IRS Breach Response Analysis to clarify that these processes constitute an evaluation of the agency's response to data breaches involving PII to identify lessons learned that are incorporated into agency security and privacy policies and practices

**IMPLEMENTATION DATE:**
December 31, 2013

**RESPONSIBLE OFFICIAL:**
Director, Privacy, Governmental Liaison & Disclosure

**CORRECTIVE ACTION MONITORING PLAN:**
We will monitor this action as part of our internal management control process.

# Appendix IX: Comments from the Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

November 22, 2013

Mr. Gregory C. Wilshusen
Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and respond to the U.S. Government Accountability Office ("GAO") draft report, *"Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent (GAO-14-34)."* We note that the report contains positive findings on the SEC's inclusion of key management and operational practices in its policies for responding to data breaches involving personally identifiable information ("PII"). We appreciate the GAO's observations of our practices. In addition, the report makes three recommendations regarding the SEC's implementation of operational steps in data breach response. The SEC offers comments as noted below regarding the recommendations and certain findings in the report.

**Recommendation 1 - Require documentation of the risk assessment performed for breaches involving PII, including the reasoning behind risk determinations:**

The SEC consistently requires and prepares meaningful risk assessment reports in accordance with guidance from the Office of Management and Budget ("OMB"). As noted in the report, 96% of SEC incidents reviewed by GAO involved lost pieces of equipment, such as BlackBerry smartphones. These devices are both securely encrypted by default and, due to active remote management, can be remotely erased in the event of loss. The SEC, as a precaution, considers lost pieces of equipment a potential breach and assesses these incidents when reported. However, because of the compensating controls, the SEC considers incidents involving encrypted equipment to be covered by a previously reported incident where the SEC assessed a low level of risk and set forth its rational for this risk determination. The SEC believes that preparing a separate risk assessment report for each incident involving encrypted, remotely managed devices does not provide meaningful value to the data breach process. The SEC continuously logs and tracks all occurrences of these types of incidents, including the 96% reviewed by GAO. Additionally, the SEC makes the required report to the United States Computer Emergency Readiness Team ("US-CERT"). The SEC's tracking documentation evidences that it consistently assessed these incidents as low risk, because of the compensating controls of encryption and remote management, and that such assessment is appropriate for the incidents involved.

Mr. Gregory C. Wilshusen
Page 2

**Recommendation 2 - Document the number of affected individuals associated with each incident involving PII:**

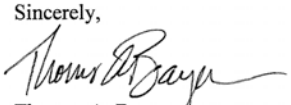
The SEC consistently documents the number of affected individuals in incidents involving PII. In incidents involving lost encrypted devices, the SEC utilizes NIST certified encryption technology, which, as per OMB Memorandum 07-16, ensures the risk of compromise is low to non-existent. As a result, the number of potentially affected individuals is immediately mitigated to a negligible number.

**Recommendation 3 – Require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices:**

As noted in the report, there is no OMB requirement to perform lessons learned exercises for data breaches and to document results of the exercise. However, the SEC consistently examines operational steps in its data breach response process, and implements new controls and IT security measures in response to lessons learned from previous privacy incidents. As a part of the five factor analysis of the privacy incident report, the SEC assesses mitigation measures and identifies security controls that could help detect, analyze, and mitigate future incidents. Recommendations are made to offices and divisions impacted—and, when applicable, to the agency as a whole—for remedial measures to prevent future occurrences. Additionally the SEC augments its privacy awareness training based on lessons learned from breach scenarios over the previous year. The SEC currently has policy requirements in place to conduct semiannual "lessons learned" reviews of it privacy incidents and the agency will comply with this policy requirement.

We appreciate the insight the GAO has provided regarding its review of issues related to PII data breaches. The SEC is committed to protecting the privacy of personal information entrusted to us. We recognize there are still opportunities for continued success. We appreciate the GAO's attention to this important issue. Thank you for the consideration that you and your staff have shown our agency.

Sincerely,



Thomas A. Bayer
Chief Information Officer and
Senior Agency Official for Privacy

# Appendix X: Comments from the Department of Veterans Affairs

**DEPARTMENT OF VETERANS AFFAIRS**
**Washington DC 20420**

NOV 25 2013

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***"Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent"*** (GAO-14-34).

The Department non-concurs with three of the GAO recommendations and concurs in principle with the fourth recommendation. VA has procedures in place for reporting to external entities which are documented in VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information, and the VA-Network Security Operations Center Incident Response Plan. The Department already documents the reasoning behind risk determinations for breaches involving personally identifiable information as well as the number of affected individuals associated with each incident in the Privacy and Security Event Tracking System. VA also regularly integrates data breach best practices into existing security and privacy policies and practices.

The Department also has concerns with several of the findings documented in GAO's draft report. For example, VA is currently unaware of any data breach or suspected data breach that has not been appropriately responded to within the guidelines of VA regulations or Federal mandates. Details are described in the enclosure that contains VA's comments to the draft report.

VA appreciates the opportunity to comment on the draft report.

Sincerely,

Jose D. Riojas
Chief of Staff

Enclosures

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
***"Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent"***
(GAO-14-34)

**GAO Recommendation: To improve the department's response to data breaches involving PII, we recommend that the Secretary of Veterans Affairs:**

**Recommendation 1: document procedures for reporting to external entities in the department's data breach response policy;**

**VA Comment:** Non-concur. These processes and procedures are already documented and implemented. The Department of Veterans Affairs (VA) data breach handbook is VA Handbook 6500.2, titled *"Management of Data Breaches Involving Sensitive Personal Information" dated January 6, 2012.* The current version of the handbook addresses VA's monthly and quarterly reporting to Congress (found in Appendix B, Table B-6 and Appendix C) and the process for HITECH Act reportable incidents (found in Appendix D). VA's reporting to the United States Computer Emergency Readiness Team (US-CERT) is documented in VA-Network Security Operations Center (NSOC) Incident Response Plan 6210.013, dated August 21, 2013 (found in Section 6.3). VA provided GAO a copy of the plan on November 21, 2013.

**Recommendation 2: require documentation of the reasoning behind risk determinations for breaches involving PII;**

**VA Comment:** Non-concur. VA currently performs these actions. For each individual incident, VA creates an entry in the Privacy and Security Event Tracking System (PSETS) which documents the reasoning behind a risk determination. VA Handbook 6500.2 clearly defines what is considered a breach and what notification is to be made to affected individuals.

While VA has processes in place that it is currently utilizing; VA has created a new Breach Criteria Document (Attachment A) and Breach Risk Assessment Tool (Attachment B) as a result of the recent Health Insurance Portability and Accountability Act Omnibus Final Rule revisions. This document outlines rules regarding mis-mailings, mis-handlings, missing/stolen equipment, e-mail, unauthorized access, improper disposal, and notification determination for breaches. The Risk Assessment Tool will be utilized as a means to determine if a particular incident meets specific breach criteria. The policy reflecting this new final rule revision has been implemented while under formal VA concurrence. This document will be incorporated into the revision of VA Handbook 6500.2. VA provided GAO copies of the Breach Criteria Document and the Breach Risk Assessment Tool (which are included in the revision of VA Handbook 6500.2) on November 21, 2013.

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
***"Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent"***
(GAO-14-34)

**Recommendation 3: document the number of affected individuals associated with each incident involving PII;**

**VA Comment:** Non-concur. VA's system for tracking data breach incidents is the PSETS. Facility Privacy Officers and Information Security Officers enter incidents into this system, and one of the fields recorded is the number of individuals impacted. When the incident is first entered in the system, this is sometimes an estimate. The Incident Resolution Team (IRT) verifies the numbers of individuals affected for incidents that are determined to be data breaches. On all incidents that are determined to be data breaches, the IRT records exactly how many individuals require notification or credit monitoring in the PSETS ticket associated with the incident.

The fields in PSETS that are used to tally the number of affected individuals are:

1. Total # of CM Offers
2. Total # of Notifications

Of the 60 random samplings of individual events provided to GAO in May 2013, 24 of the events qualified as breaches, which included the total number of CM offers and/or notifications (Attachment C). This practice has been in place since 2007.

**Recommendation 4: require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.**

**VA Comment:** Concur in principle. As a matter of routine practice, data breach best practices are shared throughout the organization. VA is formalizing existing processes in VA Handbook 6500.9, *Information Security Risk Management Tier 1 and Tier 2* (located on pages 12-14), which provides the roles and responsibilities for security risk management across the VA. This Handbook is in concurrence. In addition, VA has also issued guidance on the use of mobile devices and the requirement for encryption, which is located in VA Handbook 6500 (found in Appendix D, page D-5, and Appendix F, page F-32).

VA modifies its annual on-line privacy and information security awareness training and rules of behavior to account for events that could impact the entire Department. In addition to policy and procedure updates, VA has published Data Breach lessons learned posters that focused on the prevention of the top ten incidents. It's a combination of the events seen frequently (mis-mailing, mis-handling documents, inventory issues, etc.) and also events seen less frequently, but that do more damage (lost logbooks, lost removable media, etc.). VA also sets aside a dedicated Information Security and Privacy Awareness Week where best practices and lessons learned are conveyed to all staff and contractors.

# Appendix XI: GAO Contact and Staff Acknowledgments

## GAO Contact

Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov

## Staff Acknowledgments

In addition to the contacts named above, John de Ferrari (assistant director), Carl Barden, Marisol Cruz, Nancy Glover, Wilfred Holloway, Fatima Jahan, and David Plocher made key contributions to this report.

## 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 website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

### Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

## Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.