United States Government Accountability Office

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, April 2, 2014

# INFORMATION SECURITY

# Federal Agencies Need to Enhance Responses to Data Breaches

Statement of Gregory C. Wilshusen, Director
Information Security Issues

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.

April 2, 2014

# INFORMATION SECURITY

## Federal Agencies Need to Enhance Responses to Data Breaches

Highlights of GAO-14-487T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

## Why GAO Did This Study

The federal government collects large amounts of PII from the public, including taxpayer data, Social Security information, and patient health information. It is critical that federal agencies ensure that this information is adequately protected from data breaches, and that they respond swiftly and appropriately when breaches occur. Since 1997, GAO has designated information security as a government-wide high-risk area. Further, data breaches at federal agencies have raised concerns about the protection of PII. Federal laws and other guidance specify the responsibilities of agencies in securing their information and information systems and in responding to data breaches.

This testimony addresses federal agencies' efforts to secure their information and respond to data breaches. In preparing this statement, GAO relied primarily on previously published and ongoing work in this area.

## What GAO Recommends

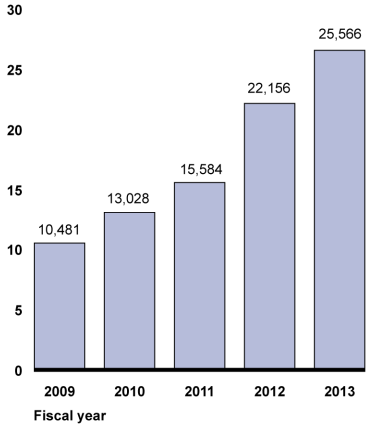
In its December 2013 report, GAO made 22 recommendations to the agencies included in its review aimed at improving their data breach response activities. GAO also recommended that OMB update its guidance on federal agencies' responses to PII-related data breaches. Agency responses to GAO's recommendations varied.

View GAO-14-487T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

## What GAO Found

The number of reported information security incidents involving personally identifiable information (PII) has more than doubled over the last several years (see figure).

**Information Security Incidents Involving PII, Fiscal Years 2009 – 2013**




Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

As GAO has previously reported, major federal agencies continue to face challenges in fully implementing all components of an agency-wide information security program, which is essential for securing agency systems and the information they contain—including PII. Specifically, agencies have had mixed results in addressing the eight components of an information security program called for by law, and most agencies had weaknesses in implementing specific security controls. GAO and inspectors general have continued to make recommendations to strengthen agency policies and practices.

In December 2013, GAO reported on agencies' responses to PII data breaches and found that they were inconsistent and needed improvement. Although selected agencies had generally developed breach-response policies and procedures, their implementation of key practices called for by Office of Management and Budget (OMB) and National Institute of Standards and Technology guidance was inconsistent. For example,

- only one of seven agencies reviewed had documented both an assigned risk level and how that level was determined for PII data breaches; two agencies documented the number of affected individuals for each incident; and two agencies notified affected individuals for all high-risk breaches.
- the seven agencies did not consistently offer credit monitoring to affected individuals; and
- none of the seven agencies consistently documented lessons learned from their breach responses.

Incomplete guidance from OMB contributed to this inconsistent implementation. For example, OMB's guidance does not make clear how agencies should use risk levels to determine whether affected individuals should be notified. In addition, the nature and timing of reporting requirements may be too stringent.

Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee:

Thank you for inviting me to testify today on efforts to protect individuals' personally identifiable information (PII)[1] from data breaches and to notify victims when a data breach has occurred. As you know, in carrying out its responsibilities the federal government collects large quantities of PII, such as taxpayer data, census data, Social Security information, and patient health information, on American citizens and other residents of our nation. Consequently, it is critical that federal agencies take steps to secure the information they collect, retain, and disseminate and that, when events such as data breaches[2] occur, they respond swiftly and appropriately. We first identified the protection of federal information systems as a government-wide high-risk area in 1997 and continued to do so in the most recent update to our high-risk series.[3]

My testimony today will discuss federal agencies' efforts to secure their information—including PII—and systems, and their responses when incidents involving PII occur. In preparing this testimony we relied on previously published work in these areas, as well as the preliminary results from a study whose results will be published later this spring. All the work supporting this statement was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

# Background

Data breaches involving PII can occur under many circumstances and for many reasons. They can be inadvertent, such as from the loss of an electronic device, or deliberate, such as from the theft of a device, or a

[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]The term "data breach" generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information, including PII.

[3]GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

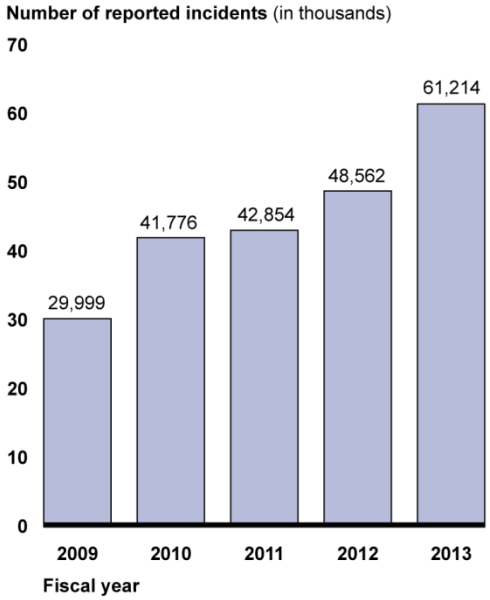
cyber-based attack by a malicious individual or group, foreign nation, terrorist, or other adversary. Incidents have been reported at a wide range of public- and private-sector institutions, including federal, state, and local government agencies; educational institutions; hospitals and other medical facilities; financial institutions; information resellers; retailers; and other types of businesses.

The loss or unauthorized disclosure or alteration of the information residing on federal systems, which can include PII, can lead to serious consequences and substantial harm to individuals and the nation. Thus it is critical that federal agencies protect their systems and the information on them and respond to data breaches and cyber incidents when they occur.

## Information Security Incidents Have Increased

Over the last several years, federal agencies have reported an increasing number of information security incidents to the U.S. Computer Emergency Readiness Team (US-CERT). These include both cyber- and non-cyber-related incidents, and many of them involved PII. Figure 1 shows that the total number of security incidents reported annually more than doubled from fiscal year 2009 to fiscal year 2013.

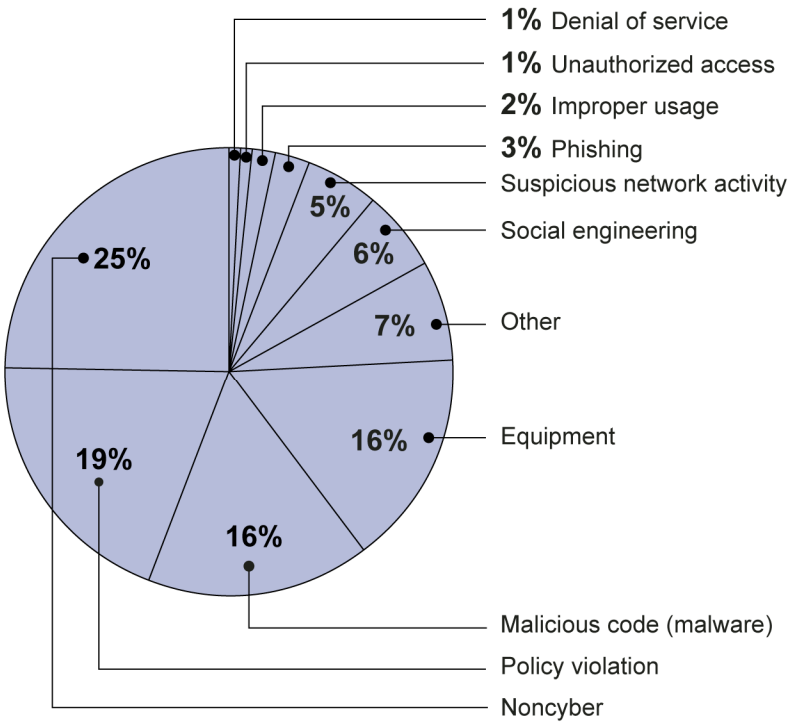
**Figure 1: Information Security Incidents Reported to US-CERT by All Federal Agencies, Fiscal Years 2009 – 2013**




Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

These incidents are categorized by type. Figure 2 shows the categories into which incidents reported in fiscal year 2013 fell.

**Figure 2: Information Security Incidents by Category, Fiscal Year 2013**

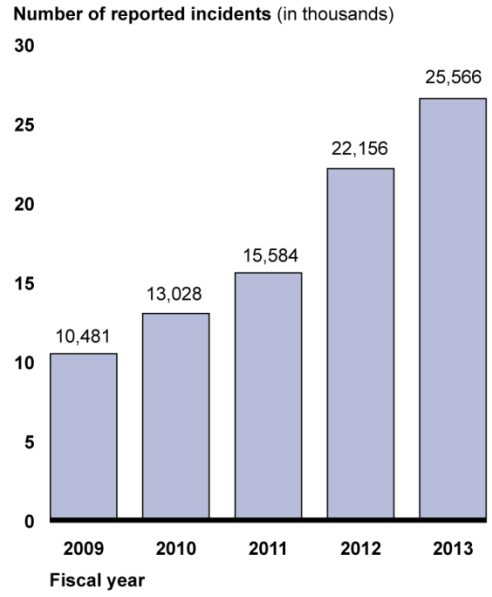



Source: GAO analysis of US-CERT data for fiscal year 2013.

Moreover, a significant number of security incidents reported by agencies have involved PII.[4] Figure 3 shows that the number of incidents involving PII for fiscal years 2009 through 2013 increased over 140 percent.

[4]PII-related incidents can include both cyber- and non-cyber-related incidents.

**Figure 3: Incidents Involving PII, Fiscal Years 2009 – 2013**




Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

Data breaches at federal agencies have received considerable publicity and raised concerns about the protection of PII at those agencies. Most notably, in May 2006, the Department of Veterans Affairs (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. More recent examples of incidents that compromised individuals' personal information further highlight the impact that such incidents can have:

- In July 2013, hackers stole a variety of PII on more than 104,000 individuals from a Department of Energy system. Types of data stolen included Social Security numbers, birth dates and locations, bank account numbers and security questions and answers. According to the department's Inspector General, the combined costs of assisting affected individuals and lost productivity—due to federal employees being granted administrative leave to correct issues stemming from the breach—could be more than $3.7 million.[5]
- In May 2012, the Federal Retirement Thrift Investment Board (FRTIB) reported a sophisticated cyber attack on the computer of a contractor

[5]Department of Energy, Office of the Inspector General, *The Department of Energy's July 2013 Cyber Security Breach*, DOE/IG-0900 (Washington, D.C.: Dec. 6, 2013).

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.

- 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 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.

## Federal Laws and Policies Establish Agency Information Security Responsibilities

Title III of the E-Government Act of 2002, known as the Federal Information Security Management Act (FISMA), establishes a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets. According to FISMA, each agency is responsible for, among other things, providing information security protections commensurate with the risk and magnitude resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor or other organization on behalf of an agency. These protections are to provide federal information and systems with integrity—preventing improper modification or destruction of information; confidentiality—preserving authorized restrictions on access and disclosure; and availability—ensuring timely and reliable access to and use of information.

Under FISMA, 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. The law also requires the operation of a central federal information security incident center that compiles and analyzes information about incidents that threaten information security. The Department of Homeland Security (DHS) was given the role of operating this center, which became US-CERT, by the

Homeland Security Act. DHS's role is further defined by Office of Management and Budget (OMB) guidance, which requires that incidents involving PII be reported to US-CERT within 1 hour of discovery. US-CERT is also responsible for providing timely technical assistance to operators of agency information systems regarding security incidents, including offering guidance on detecting and handling incidents.

In addition to establishing responsibilities for agencies, FISMA assigns specific responsibilities to OMB, the National Institute of Standards and Technology (NIST) and inspectors general:

- OMB is to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies (except with regard to national security systems). It is also responsible for reviewing, at least annually, and approving or disapproving agency information security programs.
- NIST's responsibilities include developing security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of risk levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.
- Agency inspectors general are required to annually evaluate the information security program and practices of their agency. The results of these evaluations are to be submitted to OMB, and OMB is to summarize the results in its reporting to Congress.

In July 2010, the Director of OMB and the White House Cybersecurity Coordinator issued a joint memorandum stating that DHS was to exercise primary responsibility within the executive branch for the operational aspects of cybersecurity for federal information systems that fall within the scope of FISMA.

# Agencies Continue to Face Challenges in Effectively Securing Their Information

In September 2013 we issued the most recent of our periodic reports on federal agencies' compliance with the requirements of FISMA.[6]

[6]GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*, GAO-13-776 (Washington, D.C.: Sept. 26, 2013).

Specifically, we reported that, for fiscal year 2012, 24 major federal departments and agencies covered by the Chief Financial Officers Act[7] had established many of the components of an agency-wide information security program, as required by FISMA, but had only partially established others.

In particular, with regard to the eight components of an agency-wide security program,

- 18 agencies had fully implemented a program for managing information security risk, and 6 had partially implemented such a program;
- 10 agencies had fully documented security policies and procedures, while 12 had partially documented them;[8]
- 18 agencies had selected security controls for their systems, but 6 had only partially implemented this practice;
- 22 agencies had established a security training program, and 2 had partially established such a program;
- 13 agencies were monitoring security controls on an ongoing basis, but 10 agencies had not fully implemented a continuous monitoring program;[9]
- 19 agencies had established a program for remediating weaknesses in their security policies, practices, and procedures, while 5 had not fully implemented elements of a remediation program;
- 20 agencies had established an incident response and reporting program, but 3 agencies had not fully established such a program;[10] and
- 18 agencies had fully established a program for ensuring continuity of operations in the event of a disruption or disaster, but 5 agencies partially implemented a continuity of operations program.[11]

[7]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[8]An additional 2 agencies did not fully evaluate this program component in 2012.

[9]One additional agency did not fully evaluate this program component in fiscal year 2012.

[10]One additional agency did not fully evaluate this program component in fiscal year 2012.

The extent to which the agencies had implemented security program components showed mixed progress from fiscal year 2011 to fiscal year 2012. For example, according to inspectors general reports, the number of agencies that had analyzed, validated, and documented security incidents increased from 16 to 19, while the number able to track identified weaknesses had declined from 20 to 15.

In addition, although most agencies had implemented elements of their security programs, we and inspectors general continued to identify weaknesses in elements of their programs, such as the implementation of specific security controls. Specifically, most major federal agencies had weaknesses in major categories of information security controls, as defined by our *Federal Information System Controls Audit Manual*.[12]

Table 1 shows, for fiscal year 2012, the number of the 24 major federal agencies that had weaknesses in the five major control categories.

**Table 1: Information Security Control Weaknesses at 24 Major Agencies in Fiscal Year 2012**

| Control category | Number of agencies with weaknesses |
|---|---|
| Security management | 24 |
| Access controls | 23 |
| Configuration management | 24 |
| Segregation of duties | 18 |
| Contingency planning | 24 |

Source: GAO analysis of agency inspector general data.

Note: *Security management* includes an agency-wide information security program to provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; *access controls* ensure that only authorized individuals can read, alter, or delete data; *configuration management* controls provide assurance that only authorized software programs are implemented; *segregation of duties* reduces the risk that one individual can independently perform inappropriate actions without detection; and *contingency planning* includes continuity of operations, which provides for the prevention of significant disruptions of computer-dependent operations.

Illustrating the extent to which weaknesses continue to affect the 24 major federal agencies, in fiscal year 2013, inspectors general at 21 of the 24 agencies cited information security as a major management challenge for their agency, and 18 agencies reported that information security control

[11]One additional agency did not fully evaluate this program component in fiscal year 2012.

[12]GAO, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G (Washington, D.C.: February 2009).

deficiencies were either a material weakness or significant deficiency[13] in internal controls over financial reporting in fiscal year 2013. These weaknesses show that information security continues to be a major challenge for federal agencies, putting federal systems and the information they contain, including PII, at increased risk. We and agency inspectors general have continued to make numerous recommendations to agencies aimed at improving their information security posture. Fully implementing these recommendations will strengthen agencies' ability to ensure that their information, including PII, is adequately protected.

# Agencies Need to Improve Responses to Data Breaches and Cyber Incidents

Even when information security programs have been implemented effectively, data breaches can occur. Accordingly, OMB and NIST have specified key practices for responding to PII data breaches.[14] These include *management practices* such as establishing a data breach response team and training employees on roles and responsibilities for breach response, and *operational practices*, such as preparing reports on suspected data breaches and submitting them to appropriate internal and external entities, assessing the likely risk of harm and level of impact of a suspected breach, offering assistance to affected individuals (if appropriate), and analyzing the agency's breach response and identifying lessons learned. Table 2 provides more details on these key management and operational practices.

[13]A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[14]These practices were specified in guidance documents issued by OMB and NIST. See OMB, S*afeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (Washington, D.C.: May 22, 2007); and NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

**Table 2: Key Management and Operational Practices to Be Included in Policies for Responding to Data Breaches Involving Personally Identifiable Information (PII)**

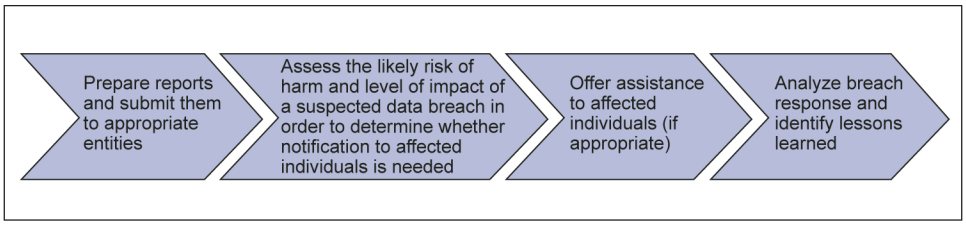
| Key management practice | Description |
|---|---|
| Establish a data breach response team | While technical remediation is usually handled by IT security staff, agencies should create a team to oversee responses to a suspected or confirmed data breach, including the program manager of the program experiencing 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 | Description |
|---|---|
| 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.

In December 2013, we reported on our review of issues related to PII data breaches.[15] The eight agencies in our review[16] had generally developed, but inconsistently implemented, policies and procedures for responding to a data breach involving PII that addressed key practices. Specifically, with few exceptions, the agencies reviewed addressed the key management and operational practices in their policies and procedures. However, they did not consistently implement the operational practices, as summarized in figure 4.

**Figure 4: Operational Steps in Data Breach Response Practices**




Source: GAO analysis of OMB and NIST guidelines.

For example,

- Of the seven agencies[17] we reviewed, only the Internal Revenue Service (IRS) consistently documented both an assigned risk level and how that level was determined for PII-related data breach incidents; only the Army and IRS documented the number of affected individuals for each incident; and only the Army and the Securities and Exchange Commission notified affected individuals for all high-risk breaches.
- The seven agencies did not consistently offer credit monitoring to individuals affected by PII-related breaches.
- None of the seven agencies consistently documented lessons learned from PII breaches, including corrective actions to prevent similar

[15]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

[16]These agencies were the Centers for Medicare & Medicaid Services, Department of the Army, Department of Veterans Affairs, Federal Deposit Insurance Corporation, Federal Reserve Board, Federal Retirement Thrift Investment Board, Internal Revenue Service, and Securities and Exchange Commission.

[17]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.

incidents in the future or whether better security controls could help detect, analyze, and mitigate future incidents.

Incomplete guidance from OMB contributed to this inconsistent implementation. For example, OMB's guidance does not make clear how agencies should use risk levels in making a determination about notification to affected individuals. Further, OMB 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.

In addition, OMB guidance for reporting on data breaches involving PII may be too stringent. Specifically, OMB guidance requires that DHS collect information about PII-related breaches within 1 hour, but officials at US-CERT and the agencies in our review generally agreed that this requirement was difficult to meet and may not provide US-CERT with the best information. For example, some agencies noted that it is difficult to provide a meaningful report on a breach within 1 hour since relevant information—such as how much PII was affected or the extent of the risk—may not be available within that time frame.

Agency officials also questioned the value of reporting certain types of PII breaches, such as paper-based incidents or incidents involving the loss of hardware containing encrypted PII, individually to US-CERT, as currently required. Officials from US-CERT agreed that their office should not be receiving all PII-related incident reports individually as they occur.

According to DHS officials, the PII-related incident data they collect are not generally used to help remediate incidents or provide technical assistance to agencies. Rather, the information is compiled in accordance with certain FISMA requirements and reported to OMB. We determined that the limited use of these data calls into question OMB's requirement that such incidents be reported within 1 hour. US-CERT officials also noted that the vast majority of PII-related data breaches are not cybersecurity related—that is, they do not involve attacks on or threats to government systems or networks. Thus receiving information about such incidents on an individual basis may not be useful to the office in pursuing its mission.

Finally, we reported that seven of the eight agencies in our review had not requested technical assistance from US-CERT when PII data breaches have occurred. DHS officials said that US-CERT is not equipped to assist agencies in remediating paper-based incidents, and agencies agreed that issues they encounter in dealing with PII breaches are generally best addressed by agency general counsel staff or privacy officers. DHS's

Privacy Office has developed guidance that addresses agencies' obligations to protect PII and procedures to follow when a suspected PII incident occurs, but this is geared more toward developing agency response capabilities in general rather than supporting decision-making related to specific incidents.

In our report, we recommended that OMB revise its guidance on federal agencies' response to PII-related data breaches to include (1) guidance on notifying affected individuals based on a determination of the level of risk; (2) criteria for determining whether to offer assistance, such as credit monitoring, to affected individuals; and (3) revised requirements for reporting PII-related breaches to US-CERT. In commenting on our draft report, officials from OMB's Office of Information and Regulatory Affairs stated that our recommendation did not sufficiently specify what supplemental guidance was needed; we subsequently revised the draft recommendation to provide greater specificity.

We also made a number of recommendations to the individual agencies in our review to improve their response to data breaches involving PII. Specifically, we recommended, among other things, that several of the agencies (1) consistently document risk levels and how those levels are determined for PII-related data breach incidents; (2) document the number of affected individuals for each incident; and (3) identify lessons learned from responses to PII breaches. Agencies varied in the extent to which they concurred with these recommendations, with some providing information pertaining to the recommendations. In response to agencies' comments, we clarified or deleted three draft recommendations but retained the rest as still warranted.

## Agencies Need to Improve Cyber Incident Response Practices

In a forthcoming report, to be issued later this spring, we plan to provide the results of our study of federal agencies' ability to respond to cyber incidents.[18] More specifically, we have determined the extent to which (1) federal agencies are effectively responding to cyber incidents, and (2) DHS is providing cybersecurity incident assistance to agencies.

While these results are still subject to revision, we estimate, based on a statistical sample of cyber incidents reported in fiscal year 2012, that the 24 major federal agencies did not effectively or consistently demonstrate actions taken in response to a detected cyber incident in about 65 percent

[18]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (forthcoming).

of reported incidents.[19] For example, agencies identified the scope of incidents in the majority of cases, but did not always demonstrate that they had determined the impact of an incident. In addition, agencies did not consistently demonstrate how they had handled other key activities, such as whether actions to prevent the recurrence of an incident were taken.

We also reviewed six selected agencies in greater depth and found that, while they had developed parts of policies, plans, and procedures to guide incident response activities, their efforts were not comprehensive or fully consistent with federal requirements. The inconsistencies in agencies' incident response activities suggest that additional oversight, such as that provided by OMB and DHS during the CyberStat review process,[20] may be warranted. However, these meetings generally have not covered agencies' incident response practices.

With regard to DHS's role, we observed that DHS provides various services to agencies to assist them in preparing to handle incidents, maintain awareness of the current threat environment, and deal with ongoing incidents addressing cyber incidents. However, opportunities exist to enhance the usefulness of these services, such as improving reporting requirements and evaluating the effectiveness of these services.

To improve the effectiveness of government-wide cyber incident response activities, we are planning to make recommendations to OMB and DHS to address agency response practices. We also plan to make recommendations to the six selected agencies in our review to improve their cyber incident response programs.

## Concluding Observations

In summary, the increasing number of cyber incidents at federal agencies, many involving the compromise of PII, highlights the need for focused agency action to ensure the security of the large amount of sensitive personal information collected by the federal government. These actions include establishing comprehensive agency-wide information security programs and consistently and effectively responding to incidents

[19]There is 95 percent confidence that the estimate falls between 58 and 72 percent.

[20]CyberStat reviews are in-depth sessions with National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration.

when they occur. As we and inspectors general have long pointed out, federal agencies continue to face challenges in effectively implementing all elements of their information security programs. Likewise, agencies have not been consistent or fully effective in responding to data breaches and cyber incidents. Ongoing improvements in these areas are needed to help ensure that the personal information entrusted to the government by American citizens and other individuals will be protected.

Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee, this concludes my statement. I would be happy to answer any questions you may have.

## Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include John A. de Ferrari and Jeffrey Knott (assistant directors), Larry E. Crosland, Marisol Cruz, and Lee McCracken.