December 2013

INFORMATION SECURITY

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

GAO Highlights

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

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.

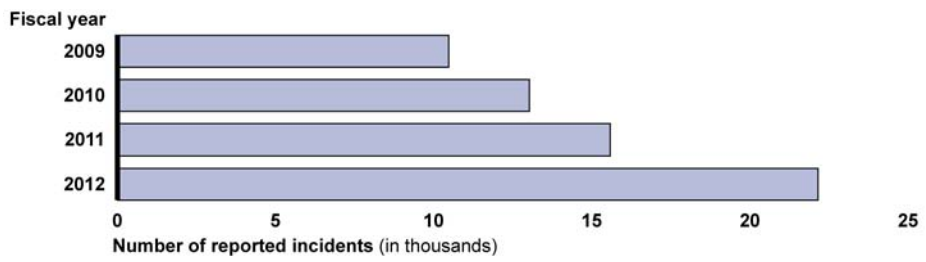
View GAO-14-34. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

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.