GAO Highlights

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.

April 2, 2014

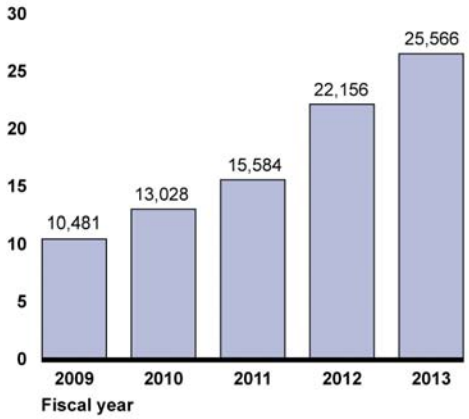
# INFORMATION SECURITY

## Federal Agencies Need to Enhance Responses to Data Breaches

## 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.