GAO Highlights

Highlights of GAO-16-194T, a testimony before the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate and the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives

November 17, 2015

INFORMATION SECURITY

Federal Agencies Need to Better Protect Sensitive Data

Why GAO Did This Study

Effective information security for federal computer systems and databases is essential to preventing the loss of resources; the unauthorized or inappropriate use, disclosure, or alteration of sensitive information; and the disruption of government operations. Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Earlier this year, in GAO's high-risk update, the area was further expanded to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

This statement summarizes threats and information security weaknesses in federal systems. In preparing this statement, GAO relied on its previously published work in this area.

What GAO Recommends

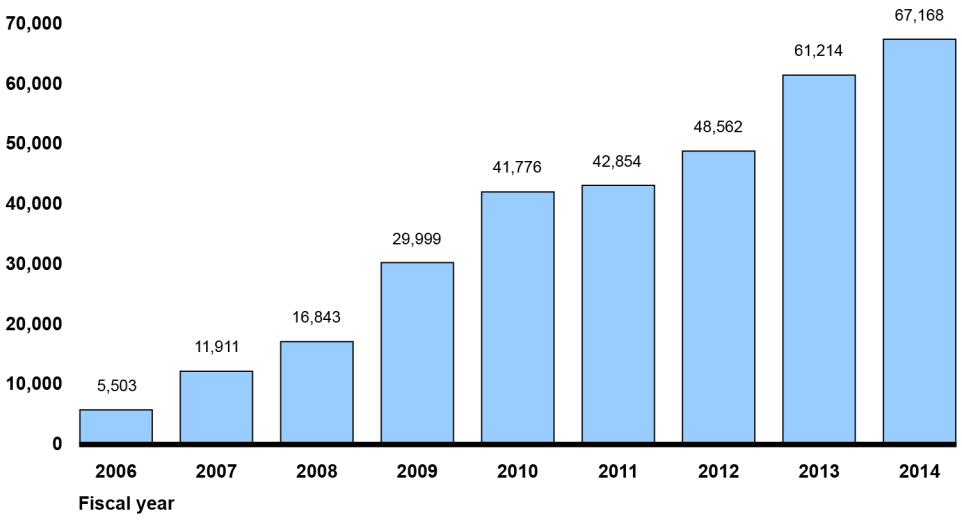
Over the past 6 years, GAO has made about 2,000 recommendations to improve information security programs and associated security controls. Agencies have implemented about 58 percent of these recommendations. Further, agency inspectors general have made a multitude of recommendations to assist their agencies.

View GAO-16-194T. For more information, contact Joel C. Willemssen at (202) 512-6253 or willemssenj@gao.gov.

What GAO Found

Federal systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from software coding errors or the actions of careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, terrorists, disgruntled employees or other organizational insiders, among others. These concerns are further highlighted by recent incidents involving breaches of sensitive data and the sharp increase in information security incidents reported by federal agencies over the last several years, which have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014 (see figure).

Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-16-194T

Security control weaknesses place sensitive data at risk. GAO has identified a number of deficiencies at federal agencies that pose threats to their information and systems. For example, agencies, including the Department of Homeland Security, have weaknesses with the design and implementation of information security controls, as illustrated by 19 of 24 agencies covered by the *Chief Financial Officers Act* declaring cybersecurity as a significant deficiency or material weakness for fiscal year 2014. In addition, most of the 24 agencies continue to have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware.

Until federal agencies take actions to address these weaknesses—including implementing the thousands of recommendations GAO and agency inspectors general have made—federal systems and information will be at an increased risk of compromise from cyber-based attacks and other threats.