November 17, 2015

INFORMATION SECURITY

Department of Education and Other Federal Agencies Need to Better Implement Controls

GAO Highlights

Highlights of GAO-16-228T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The federal government faces an evolving array of cyber-based threats to its systems and data, and data breaches at federal agencies have compromised sensitive personal information, affecting millions of people. Education, in carrying out its mission of serving America's students, relies extensively on IT systems that collect and process a large amount of sensitive information. Accordingly, it is important for federal agencies such as Education to implement information security programs that can help protect systems and networks. GAO has identified federal information security as a government-wide high-risk area since 1997, and in February 2015 expanded this to include protecting the privacy of personally identifiable information.

This statement provides information on cyber threats facing federal systems and information security weaknesses identified at federal agencies, including Education. In preparing this statement, GAO relied on previously published work and updated data on security incidents and federal cybersecurity efforts.

What GAO Recommends

Over the past 6 years, GAO has made about 2,000 recommendations to federal agencies to correct weaknesses and fully implement agency-wide information security programs. Agencies have implemented about 58 percent of these recommendations. Agency inspectors general have also made a multitude of recommendations to assist their agencies.

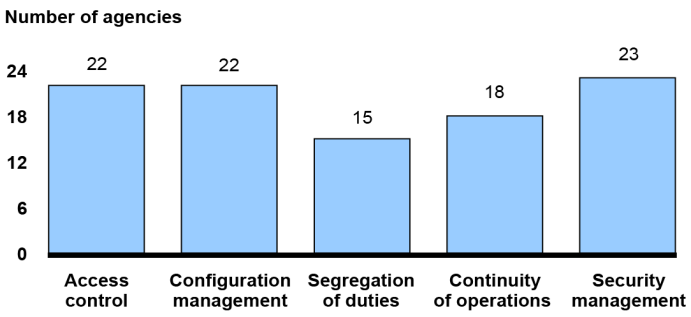
View GAO-16-228T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber-based risks to federal systems and information can come from unintentional threats, such as natural disasters, software coding errors, and poorly trained or careless employees, or intentional threats, such as disgruntled insiders, hackers, or hostile nations. These threat sources may exploit vulnerabilities in agencies' systems and networks to steal or disclose sensitive information, among other things. Since fiscal year 2006, the number of reported information security incidents affecting federal systems has steadily increased, rising from about 5,500 in fiscal year 2006 to almost 67,200 in fiscal year 2014. At the Department of Education, the number of incidents reported since 2009 has fluctuated, but generally increased.

GAO reported in September 2015, that most of 24 major agencies (including Education) had weaknesses in at least three of five major categories of information security controls for fiscal year 2014. These are controls intended to (1) limit unauthorized access to agency systems and information; (2) ensure that software and hardware are authorized, updated, monitored, and securely configured; (3) appropriately divide duties so that no single person can control all aspects of a computer-related operation; (4) establish plans for continuing information system operations in the event of a disaster, and (5) provide a security management framework for understanding risks and ensuring that controls are selected, implemented, and operating as intended. The figure below shows the number of agencies with weaknesses in these control categories.

Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agency, inspector general, and GAO reports as of May 2015. | GAO-16-228T

In addition, 19 agencies—including Education—reported that information security control deficiencies were either a material weakness or a significant deficiency for fiscal year 2014. Further, inspectors general for 23 of 24 agencies, including Education, cited information security as a major management challenge. In prior reports, GAO and inspectors general have made thousands of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain open. Until agencies implement these recommendations, sensitive information will remain at risk of unauthorized disclosure, modification, or destruction.