GAO Highlights

Highlights of GAO-16-501, a report to congressional requesters

May 2016

INFORMATION SECURITY

Agencies Need to Improve Controls over Selected High-Impact Systems

Why GAO Did This Study

Federal systems categorized as high impact—those that hold sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harm—warrant increased security to protect them. In this report, GAO (1) describes the extent to which agencies have identified cyber threats and have reported incidents involving high-impact systems, (2) identifies government-wide guidance and efforts to protect these systems, and (3) assesses the effectiveness of controls to protect selected high-impact systems at federal agencies. To do this, GAO surveyed 24 federal agencies; examined federal policies, standards, guidelines and reports; and interviewed agency officials. In addition, GAO tested and evaluated the security controls over eight high-impact systems at four agencies.

What GAO Recommends

GAO recommends that OMB complete its plans and practices for securing federal systems and that NASA, NRC, OPM, and VA fully implement key elements of their information security programs. The agencies generally concurred with GAO's recommendations, with the exception of OPM. OPM did not concur with the recommendation regarding evaluating security control assessments. GAO continues to believe the recommendation is warranted.

In separate reports with limited distribution, GAO is making specific recommendations to each of the four agencies to mitigate identified weaknesses in access controls, patch management, and contingency planning.

View GAO-16-501. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

In GAO's survey of 24 federal agencies, the 18 agencies having high-impact systems identified cyber attacks from "nations" as the most serious and most frequently-occurring threat to the security of their systems. These agencies also noted that attacks delivered through e-mail were the most serious and frequent. During fiscal year 2014, 11 of the 18 agencies reported 2,267 incidents affecting their high-impact systems, with almost 500 of the incidents involving the installation of malicious code.

Government entities have provided guidance and established initiatives and services to aid agencies in protecting their systems, including those categorized as high impact. The National Institute of Standards and Technology has prescribed federal standards for minimum security requirements and guidance on security and privacy controls for high-impact systems, including 83 controls specific to such systems. The Office of Management and Budget (OMB) is developing plans for shared services and practices for federal security operations centers but has not issued them yet. In addition, agencies reported that they are in the process of implementing various federal initiatives, such as tools to diagnose and mitigate intrusions on a continuous basis and stronger controls over access to agency networks.

The National Aeronautics and Space Administration (NASA), Nuclear Regulatory Commission (NRC), Office of Personnel Management (OPM), and Department of Veterans Affairs (VA) had implemented numerous controls over the eight high-impact systems GAO reviewed. For example, all the agencies reviewed had developed a risk assessment for their selected high-risk systems. However, the four agencies had not always effectively implemented access controls. These control weaknesses included those protecting system boundaries, identifying and authenticating users, authorizing access needed to perform job duties, and auditing and monitoring system activities. Weaknesses also existed in patching known software vulnerabilities and planning for contingencies. An underlying reason for these weaknesses is that the agencies had not fully implemented key elements of their information security programs, as shown in the table.

Agency Implementation of Key Information Security Program Elements for Selected Systems

	NASA	NRC	OPM	VA
Risk assessments	●	●	●	●
Security plans	●	◐	◐	◐
Controls assessments	◐	◐	◐	○
Remedial action plans	◐	◐	◐	◐

Source: GAO analysis of agency documentation. | GAO-16-501

Note: ● – Met ◐ – Partially met ○ – Did not meet

Until the selected agencies address weaknesses in access and other controls, including fully implementing elements of their information security programs, the sensitive data maintained on selected systems will be at increased risk of unauthorized access, modification, and disclosure, and the systems at risk of disruption.