December 2018

INFORMATION SECURITY

Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions

GAO Highlights

Highlights of GAO-19-105, a report to congressional committees

Why GAO Did This Study

Federal agencies are dependent on information systems to carry out operations. The risks to these systems are increasing as security threats evolve and become more sophisticated. To reduce the risk of a successful cyberattack, agencies can deploy intrusion detection and prevention capabilities on their networks and systems.

GAO first designated federal information security as a government-wide high-risk area in 1997. In 2015, GAO expanded this area to include protecting the privacy of personally identifiable information. Most recently, in September 2018, GAO updated the area to identify 10 critical actions that the federal government and other entities need to take to address major cybersecurity challenges.

The federal approach and strategy for securing information systems is grounded in the provisions of the *Federal Information Security Modernization Act of 2014* and Executive Order 13800. The act requires agencies to develop, document, and implement an agency-wide program to secure their information systems. The Executive Order, issued in May 2017, directs agencies to use the National Institute of Standards and Technology's cybersecurity framework to manage cybersecurity risks.

The *Federal Cybersecurity Enhancement Act of 2015* contained a provision for GAO to report on the effectiveness of the government's approach and strategy for securing its systems. GAO determined (1) the reported effectiveness of agencies'

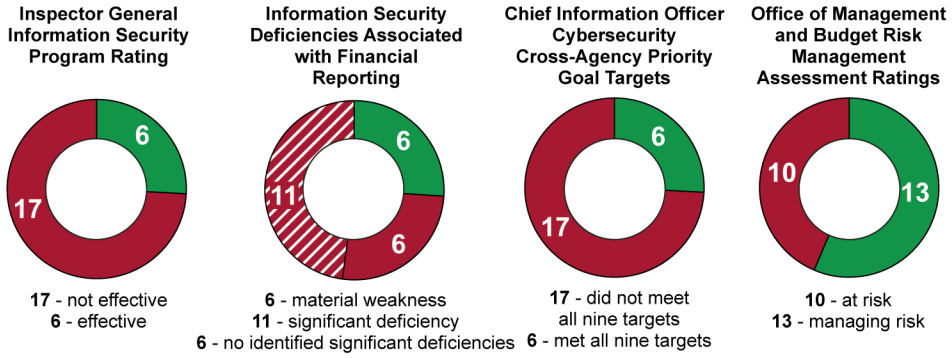
View GAO-19-105. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* (CFO Act) have often not effectively implemented the federal government's approach and strategy for securing information systems (see figure below). Until agencies more effectively implement the government's approach and strategy, federal systems will remain at risk. To illustrate:

- As required by Office of Management and Budget (OMB), inspectors general (IGs) evaluated the maturity of their agencies' information security programs using performance measures associated with the five core security functions—identify, protect, detect, respond, and recover. The IGs at 17 of the 23 agencies reported that their agencies' programs were not effectively implemented.
- IGs also evaluated information security controls as part of the annual audit of their agencies' financial statements, identifying material weaknesses or significant deficiencies in internal controls for financial reporting at 17 of the 23 civilian CFO Act agencies.
- Chief information officers (CIOs) for 17 of the 23 agencies reported not meeting all elements of the government's cybersecurity cross-agency priority goal. The goal was intended to improve cybersecurity performance through, among other things, maintaining ongoing awareness of information security, vulnerabilities, and threats; and implementing technologies and processes that reduce malware risk.
- Executive Order 13800 directed OMB, in coordination with the Department of Homeland Security (DHS), to assess and report on the sufficiency and appropriateness of federal agencies' processes for managing cybersecurity risks. Using performance measures for each of the five core security functions, OMB determined that 13 of the 23 agencies were managing overall enterprise risks, while the other 10 agencies were at risk. In assessing agency risk by core security function, OMB identified a few agencies to be at high risk (see figure at the top of next page).

Fiscal Year 2017 Indicators of the 23 Selected Civilian Agencies' Effectiveness in Implementing the Federal Approach and Strategy for Securing Information Systems



Source: GAO analysis of agency fiscal year 2017 *Federal Information Security Modernization Act of 2014* and agency financial reports for fiscal year 2017. | GAO-19-105

Why GAO Did This Study (cont.)

implementation of the government's approach and strategy; (2) the extent to which DHS and OMB have taken steps to facilitate the use of intrusion detection and prevention capabilities to secure federal systems; and (3) the extent to which agencies reported implementing capabilities to detect and prevent intrusions.

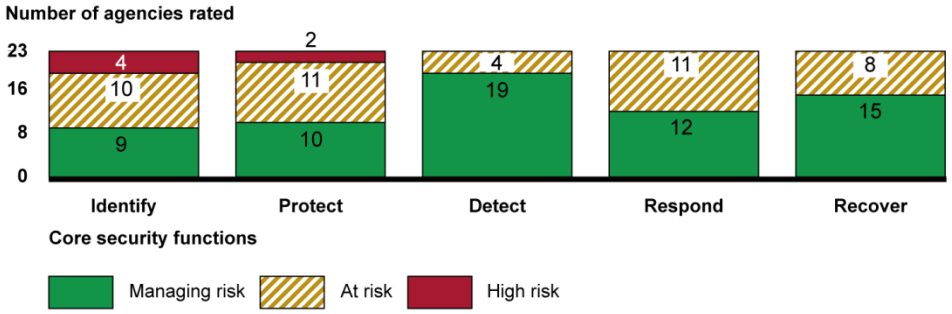
To address these objectives, GAO analyzed OMB reports related to agencies' information security practices including OMB's annual report to Congress for fiscal year 2017. GAO also analyzed and summarized agency-reported security performance metrics and IG-reported information for the 23 civilian CFO Act agencies. In addition, GAO evaluated plans, reports, and other documents related to DHS intrusion detection and prevention programs, and interviewed OMB, DHS, and agency officials.

What GAO Recommends

GAO is making two recommendations to DHS, to among other things, coordinate with agencies to identify additional needs for training and guidance. GAO is also making seven recommendations to OMB to, among other things, direct the Federal CIO to update the mandated report with required information, such as detecting advanced persistent threats. DHS concurred with GAO's recommendations. OMB did not indicate whether it concurred with the recommendations or not.

What GAO Found (cont.)

Risk Management Assessment Ratings by Core Security Function for the 23 Civilian *Chief Financial Officers Act of 1990* Agencies, Fiscal Year 2017



Source: GAO analysis of Office of Management and Budget Fiscal Year 2017 *Federal Information Security Modernization Act of 2014 Annual Report To Congress.* | GAO-19-105

DHS and OMB facilitated the use of intrusion detection and prevention capabilities to secure federal agency systems, but further efforts remain. For example, in response to prior GAO recommendations, DHS had improved the capabilities of the National Cybersecurity Protection System (NCPS), which is intended to detect and prevent malicious traffic from entering agencies' computer networks. However, the system still had limitations, such as not having the capability to scan encrypted traffic. The department was also in the process of enhancing the capabilities of federal agencies to automate network monitoring for malicious activity through its Continuous Diagnostics and Mitigation (CDM) program. However, the program was running behind schedule and officials at most agencies indicated the need for additional training and guidance. Further, the Federal CIO issued a mandated report assessing agencies' intrusion detection and prevention capabilities, but the report did not address required information, such as the capability of NCPS to detect advanced persistent threats, and a cost/benefit comparison of capabilities to commercial technologies and tools.

Selected agencies had not consistently implemented capabilities to detect and prevent intrusions into their computer networks. Specifically, the agencies told GAO that they had not fully implemented required actions for protecting email, cloud services, host-based systems, and network traffic from malicious activity. For example, 21 of 23 agencies had not, as of September 2018, sufficiently enhanced email protection through implementation of DHS' directive on enhanced email security. In addition, less than half of the agencies that use cloud services reported monitoring these services. Further, most of the selected 23 agencies had not fully implemented the tools and services available through the first two phases of DHS's CDM program. Until agencies more thoroughly implement capabilities to detect and prevent intrusions, federal systems and the information they process will be vulnerable to malicious threats.