GAO Highlights

Highlights of GAO-16-686, a report to congressional requesters

August 2016

FEDERAL CHIEF INFORMATION SECURITY OFFICERS

Opportunities Exist to Improve Roles and Address Challenges to Authority

Why GAO Did This Study

Federal agencies face an ever-increasing array of cyber threats to their information systems and information. To address these threats, FISMA 2014 requires agencies to designate a CISO—a key position in agency efforts to manage information security risks.

GAO was asked to review current CISO authorities. This report identifies (1) the key responsibilities of federal CISOs established by federal law and guidance and the extent to which federal agencies have defined the role of the CISO in accordance with law and guidance and (2) key challenges of federal CISOs in fulfilling their responsibilities. GAO reviewed agency security policies, administered a survey to 24 CISOs, interviewed current CISOs, and spoke with officials from OMB.

What GAO Recommends

GAO is making 33 recommendations to 13 agencies to fully define the role of their CISOs in accordance with FISMA 2014. Twelve of the 13 agencies concurred with the recommendations addressed to them. One agency partially concurred or did not concur with the recommendations directed to it. GAO continues to believe that these recommendations are valid and should be implemented as discussed in this report. GAO also recommends that OMB issue guidance for clarifying CISOs' roles in light of identified challenges. OMB partially concurred with the recommendation. GAO maintains that action is needed as discussed further in the report.

View GAO-16-686. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Under the Federal Information Security Modernization Act of 2014 (FISMA 2014), the agency chief information security officer (CISO) has the responsibility to ensure that the agency is meeting the requirements of the law, including developing, documenting, and implementing the agency-wide information security program. However, 13 of the 24 agencies GAO reviewed had not fully defined the role of their CISO in accordance with these requirements. For example, these agencies did not always identify a role for the CISO in ensuring that security controls are periodically tested; procedures are in place for detecting, reporting, and responding to security incidents; or contingency plans and procedures for agency information systems are in place. Thus, CISOs' ability to effectively oversee these agencies' information security activities can be limited.

The 24 CISOs GAO surveyed identified challenges that limited their authority to carry out their responsibilities to oversee information security activities. These challenges can impact agencies' ability to effectively manage information security risk. The table below shows the factors that CISOs reported as being the most challenging to their authority.

Extent to Which 24 Chief Information Security Officers Reported Factors as Challenging to Their Authority

Factor	Large extent	Moderate extent	Small extent	Not at all	No response
Competing priorities between operations and security	6	12	4	2	0
Coordination with component organizations	5	8	4	5	2
Coordination with other offices	3	9	3	9	0
Availability of information from contractors	4	8	10	2	0
Oversight of indirect reports	6	6	6	6	0
Oversight of IT contractors	4	8	6	6	0
Placement in organizational hierarchy	5	5	5	9	0
Availability of information from component organizations	5	4	10	5	0

Source: GAO analysis of survey data. | GAO-16-686

The 24 CISOs also reported that other factors posed challenges to their abilities to carry out their responsibilities effectively, including difficulties related to having sufficient staff; recruiting, hiring, and retaining security personnel; ensuring that security personnel have appropriate expertise and skills; and a lack of sufficient financial resources. Several government-wide activities are under way to address many of these challenges. However, while the Office of Management and Budget (OMB) has a statutory responsibility under FISMA 2014 to provide guidance on information security in federal agencies, it has not issued such guidance addressing how agencies should ensure that officials carry out their responsibilities and personnel are held accountable for complying with the agency-wide information security program. As a result, agencies lack clarity on how to ensure that their CISOs have adequate authority to effectively carry out their duties in the face of numerous challenges.