July 2019

CYBERSECURITY

Agencies Need to Fully Establish Risk Management Programs and Address Challenges

GAO Highlights

Highlights of GAO-19-384, a report to congressional requesters

Why GAO Did This Study

Federal agencies face a growing number of cyber threats to their systems and data. To protect against these threats, federal law and policies emphasize that agencies take a risk-based approach to cybersecurity by effectively identifying, prioritizing, and managing their cyber risks. In addition, OMB and DHS play important roles in overseeing and supporting agencies' cybersecurity risk management efforts.

GAO was asked to review federal agencies' cybersecurity risk management programs. GAO examined (1) the extent to which agencies established key elements of a cybersecurity risk management program; (2) what challenges, if any, agencies identified in developing and implementing cybersecurity risk management programs; and (3) steps OMB and DHS have taken to meet their risk management responsibilities and address any challenges agencies face. To do this, GAO reviewed policies and procedures from 23 civilian *Chief Financial Officers Act of 1990* agencies and compared them to key federal cybersecurity risk management practices, obtained agencies' views on challenges they faced, identified and analyzed actions taken by OMB and DHS to determine whether they address agency challenges, and interviewed responsible agency officials.

What GAO Recommends

GAO is making 57 recommendations to the 23 agencies and one to OMB, in coordination with DHS, to assist agencies in addressing challenges. Seventeen agencies agreed with the recommendations, one partially agreed, and four, including OMB, did not state whether they agreed or disagreed. GAO continues to believe all its recommendations are warranted.

View GAO-19-384. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

Key practices for establishing an agency-wide cybersecurity risk management program include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management (ERM) program. Although the 23 agencies GAO reviewed almost always designated a risk executive, they often did not fully incorporate other key practices in their programs:

- Twenty-two agencies established the role of cybersecurity risk executive, to provide agency-wide management and oversight of risk management.
- Sixteen agencies have not fully established a cybersecurity risk management strategy to delineate the boundaries for risk-based decisions.
- Seventeen agencies have not fully established agency- and system-level policies for assessing, responding to, and monitoring risk.
- Eleven agencies have not fully established a process for assessing agency-wide cybersecurity risks based on an aggregation of system-level risks.
- Thirteen agencies have not fully established a process for coordinating between their cybersecurity and ERM programs for managing all major risks.

Until they address these practices, agencies will face an increased risk of cyber-based incidents that threaten national security and personal privacy.

Agencies identified multiple challenges in establishing and implementing cybersecurity risk management programs (see table).

Agency Challenges in Establishing Cybersecurity Risk Management Programs

Challenge	Agencies reporting challenge
Hiring and retaining key cybersecurity management personnel	23
Managing competing priorities between operations and cybersecurity	19
Establishing and implementing consistent policies and procedures	18
Establishing and implementing standardized technology capabilities	18
Receiving quality risk data	18
Using federal cybersecurity risk management guidance	16
Developing an agency-wide risk management strategy	15
Incorporating cyber risks into enterprise risk management	14

Source: GAO analysis of agency data. | GAO-19-384

In response to a May 2017 executive order, the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) identified areas for improvement in agencies' capabilities for managing cyber risks. Further, they have initiatives under way that should help address four of the challenges identified by agencies—hiring and retention, standardizing capabilities, receiving quality risk data, and using guidance. However, OMB and DHS did not establish initiatives to address the other challenges on managing conflicting priorities, establishing and implementing consistent policies, developing risk management strategies, and incorporating cyber risks into ERM. Without additional guidance or assistance to mitigate these challenges, agencies will likely continue to be hindered in managing cybersecurity risks.