GAO Highlights

Highlights of GAO-20-256T, a testimony before the Subcommittee on Technology Modernization, Committee on Veterans' Affairs, House of Representatives

November 14, 2019

INFORMATION SECURITY

VA and Other Federal Agencies Need to Address Significant Challenges

Why GAO Did This Study

In providing health care and other benefits to veterans and their dependents, VA relies extensively on IT systems and networks to receive, process, and maintain sensitive data, including veterans' medical records and other personally identifiable information. Accordingly, effective security controls based on federal guidance and requirements are essential to ensure that VA's systems and information are adequately protected from loss, unauthorized disclosure, inadvertent or deliberate misuse, or improper modification, and are available when needed.

For this testimony, GAO summarized the status of information security across the federal government and particularly at VA. It also discusses the security challenges that VA faces as it modernizes and secures its information systems. To develop this statement, GAO reviewed its prior reports and relevant Office of Management and Budget, IG, and agency reports.

What GAO Recommends

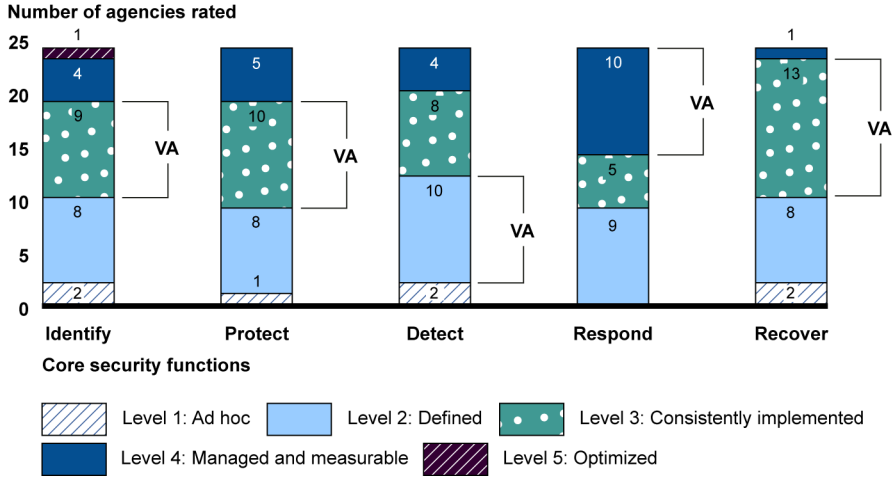
In 2016, GAO recommended 74 actions for VA to take to address deficiencies and improve its cybersecurity program. However, as of October 2019, VA had not demonstrated that it had addressed 42 of these recommendations. In 2019, GAO made four additional recommendations to improve the department's cybersecurity risk management program and one recommendation to accurately identify work roles of IT and cybersecurity workforce positions. VA concurred with these recommendations and planned to implement them.

View GAO-20-256T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies, including the Department of Veterans Affairs (VA), continue to have deficient information security programs. For example, in fiscal year 2018, inspectors general (IGs) used a five-level maturity model to rate agency information security policies, procedures, and practices related to the five core security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—established by the National Institute of Standards and Technology's cybersecurity framework. VA's ratings were generally consistent with the ratings of other major agencies (see figure) and its information security program was one of 18 agency programs that IGs deemed ineffective.

Maturity Level Ratings for the Cybersecurity Framework Core Security Functions for 24 Major Agencies, including the Department of Veterans Affairs (VA), for Fiscal Year 2018



Source: GAO analysis of agency fiscal year 2018 *Federal Information Security Modernization Act of 2014* (FISMA) reports and the Office of Management and Budget's *Fiscal Year 2018 Annual FISMA Report to Congress*. | GAO-20-256T

Most major agencies, including VA, had significant security control deficiencies over their financial reporting. For example, for fiscal year 2018, VA's IG reported deficiencies in control areas, such as security management, access control, configuration management, segregation of duties, and contingency planning. Additionally, as of fiscal year 2018, VA reported meeting six of the 10 cybersecurity performance targets set by the administration.

VA faces several security challenges as it secures and modernizes its information systems. These challenges pertain to effectively implementing information security controls; mitigating known vulnerabilities; establishing elements of its cybersecurity risk management program; and identifying critical cybersecurity staffing needs. VA also faces the additional challenge of managing IT supply chain risks as the department takes steps to modernize its information systems.