GAO Highlights

Highlights of GAO-18-201, a report to the Chairman, Committee on Veterans' Affairs, House of Representatives

January 2018

VA FACILITY SECURITY

Policy Review and Improved Oversight Strategy Needed

Why GAO Did This Study

The Veterans Health Administration (VHA is responsible for providing a safe and secure, yet welcoming environment for staff, patients, and visitors at nearly 170 medical centers. These facilities have been the target of violence, threats, and other security-related incidents. Assessing and managing risks a critical element for ensuring adequate physical security at these facilities.

GAO was asked to review VA's physical security risk-management policies and practices. This report: (1) assesses how VA's policies for risk management reflect prevailing standards, and (2) evaluates VA's oversight of risk management at VHA medical facilities. GAO compared VA policies to ISC standards; reviewed VA documents; interviewed VA and ISC officials; and assessed risk assessment activities at nine medical centers selected based on factors such as patient and security-incident data and geographical diversity. While not generalizable, these nine locations provide illustrative examples of how VA's policies are carried out.

What GAO Recommends

GAO recommends that the Department of Veterans Affairs review and revise its risk management policies to reflect prevailing standards, and develop an oversight strategy to assess the effectiveness of risk management programs at VHA facilities. VA agreed with GAO's recommendations and identified steps to implement them.

View GAO-18-201. For more information, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov

What GAO Found

The Department of Veterans Affairs' (VA) risk management policies include some but not all of the elements of standards set by the Interagency Security Committee (ISC). ISC was established via executive order to develop security standards and best practices that federal agencies are to follow when developing and conducting risk assessments. As part of this process, VA's policy identifies minimum countermeasures as called for in ISC's standards. In other areas, VA policy only partially adheres or does not adhere to ISC's standards, for example:

- Of the five factors ISC calls for when calculating a facility's security level, VA considers three but does not consider a facility's population and size.
- VA policy does not include performance measures, such as the number of countermeasures in use or the percentage of facility assessments completed; this percentage is a key element of ISC's standards for assessing the effectiveness of an agency's security programs.

Officials at VA said that its risk management program was developed prior to the ISC standards' being issued in 2013 and that it is up to each agency to determine how to best apply the standards. Nevertheless, VA officials said they are currently reexamining their policies. Until VA reviews its policies in accordance with ISC standards, its approach to risk management may not yield the appropriate security posture needed to adequately protect its medical centers.

VA's oversight activities for risk management do not encompass key aspects of the *Standards for Internal Control in the Federal Government* and *Circular A-123* from the Office of Management and Budget that require agencies to conduct oversight activities to ensure the accountability and effectiveness of agency programs. VA has an oversight process to ensure that biennial assessments of individual facilities' security are completed. However, VA:

- does not review the quality of medical centers' required risk assessments,
- does not identify whether countermeasures were implemented appropriately by the medical centers, and
- does not collect system-wide data to gain an understanding of physical security issues across medical centers.

In the absence of a comprehensive VA-wide strategy or guidance that reflects these internal control standards, individual sites have established their own approaches to carrying out VA's risk management policy. For example, the nine sites GAO reviewed conducted their security assessments differently, and none of the assessments indicated that all of the threat categories in VA's policy were reviewed. The lack of a system-wide oversight strategy means that the differences among medical center approaches, along with the security effects of those different approaches, are unknown. Accordingly, VA does not know if its medical centers are adequately protected, and it may be missing opportunities to leverage resources nationally and make better informed, proactive policy decisions.