United States Government Accountability Office

Report to the Chairman, Committee on Veterans' Affairs, House of Representatives

January 2018

VA FACILITY SECURITY

Policy Review and Improved Oversight Strategy Needed

Accessible Version

GAO-18-201

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.

Contents

Figures

Abbreviations

ERM	enterprise risk management
FSL	facility security level
ISC	Interagency Security Committee
OSLE	Office of Security and Law Enforcement
the ISC Standard	Risk Management Process for Federal Facilities (of the ISC)
UCR	Unified Crime Report
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network
VASP	Veterans Affairs Police System

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 11, 2018

The Honorable David P. Roe, M.D.
Chairman
Committee on Veterans' Affairs
House of Representatives

Dear Mr. Roe:

The Department of Veterans Affairs' (VA) Veterans Health Administration (VHA) provides critical health services to approximately 9-million enrolled veterans at its nearly 170 medical centers.[1] In recent years, however, these facilities have been the target of violence, threats, and other security-related incidents—including bomb threats and violent attacks involving weapons. For example, in 2015, a psychologist was fatally shot while working at a VA medical clinic. Ensuring physical security for these medical centers can be complicated because VA has to balance safety and security with providing an open and welcoming health-care environment. Furthermore, VA serves a vulnerable population with high rates of post-traumatic stress disorder and substance abuse.

VHA is responsible for physical security at its facilities and has issued policies and standards that the facilities must follow when assessing physical security risks. To fulfill this responsibility, VHA conducts a range of activities such as performing risk assessments, implementing countermeasures designed to minimize risks, and providing law enforcement services through VA police departments. To help agencies such as VA with their physical security, the Interagency Security Committee (ISC) issued standards for risk management of federal facilities, and agencies are supposed to follow the standards.[2]

You asked us to examine how VA ensures it is providing a secure environment at VHA facilities. This report:

[1]The total number of veteran enrollees in VA's health care system rose from 7.9 million to almost 9 million from fiscal year 2006 through fiscal year 2016.

[2]The ISC, housed within the Department of Homeland Security, includes a membership of senior level executives from 60 federal agencies and departments

- assesses the extent to which VA's policies for managing risk related to physical security reflect key elements of ISC's risk management standards, and
- evaluates VA's oversight of risk management for physical security at VHA's various facilities.

To assess how VA policies for physical security-risk management reflect key elements of ISC's risk management standards, we reviewed VA's policies pertinent to its risk management process and its risk assessment methodology and compared the policies to ISC's risk management standards.[3] This process included reviewing the Risk Management Process for Federal Facilities (ISC Standard) for assessing physical security and providing recommended countermeasures at federal facilities.[4] To assess VA's oversight of risk management of physical security at VHA facilities, we identified and examined oversight and management mechanisms at the national, regional, and local levels, including reporting mechanisms that prioritize or track facility risks or the implementation of countermeasures at VHA facilities. We also reviewed VA's oversight activities against Standards for Internal Control in the Federal Government, because internal controls play a significant role in helping agencies achieve their mission-related responsibilities using proper oversight mechanisms.[5] In addition, we reviewed VHA police responsibilities for physical security and law enforcement, including conducting risk assessments and identifying needed countermeasures.

As part of our review, we selected nine VHA medical centers to include a range of patient volumes, rates of security incidents per patient, and locations, among other considerations. For each of these medical centers, we

[3]We examined policies issued by VA's Office of Security and Law Enforcement (OSLE) as these policies form the primary mechanism for VA's risk management process (i.e., process for assessing, responding, and monitoring physical security risks) at VA facilities. Additionally, VA OSLE policies are directed at VA police, who serve as VA's security organization and are responsible for performing facility risk assessments (which VA refers to as "vulnerability assessments.")

[4]ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D. C.: November 2016).

[5]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D. C.: September 2014).

- assessed the most recent physical security documents and risk management efforts,
- reviewed the data and reporting mechanisms used to prioritize and track facility risks and the implementation of countermeasures at VHA facilities, and
- conducted semi-structured interviews with VA police, facility directors, and union representatives at these medical centers.

These steps enabled us to identify: (1) the officials' approach to physical security, (2) which countermeasures were adopted, and (3) what additional countermeasures or other efforts, if any, remain to be implemented. While the results from these nine medical centers are not generalizable to all VA medical centers, they provide illustrative examples of how the department's risk assessment policies are being implemented as well as a range of perspectives on physical security activities. See appendix I for more details on our scope and methodology.

We conducted this performance audit from September 2016 to January 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

VA has faced a growing demand by veterans for its health care services, due in part to both service members returning from military operations in Afghanistan and Iraq and to the growing needs of an aging veteran population.[6] As part of providing care to millions of veterans, VA is expected to provide a safe environment not only for the veterans, but also for staff and visitors at a diverse makeup of VHA facilities.

[6]We added managing risks and improving VA health care to our High Risk List in 2015 due to our concern about VA's ability to ensure the cost-effective and efficient use of resources to improve the timeliness, quality, and safety of health care for veterans. GAO, *High Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015). We expressed continued concerns about VA health care in our 2017 high-risk report. GAO, *High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

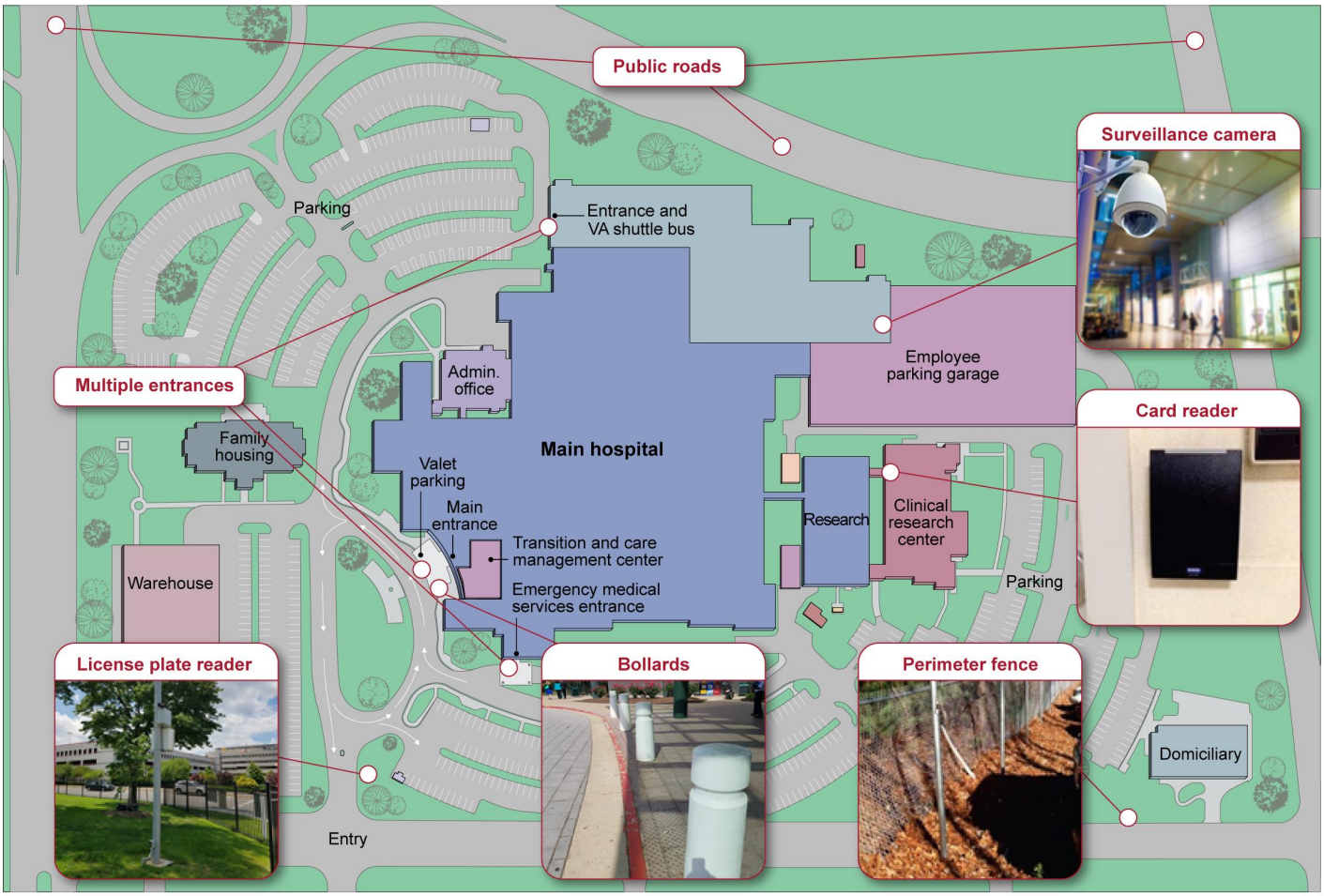
Although many of these facilities face similar challenges, differences in facilities may require different levels and types of security. For example, medical centers with large numbers of staff, patients, and visitors may require more resources for securing the facility compared to smaller medical centers with fewer people frequenting the facility daily. Some medical centers are located in densely populated urban areas, while others are located in non-urban areas, and their security challenges may differ. For example, facilities in urban areas may be located near busy public roads, making it more difficult to implement physical security enhancements such as barriers or setbacks from the street.[7] Furthermore, some VHA medical centers consist of a single hospital and others may include a campus with many buildings. According to VA officials, these differences can lead to unique security challenges. Medical centers offer different types of services, which can influence the types of security required.[8] For example, officials from multiple medical centers we reviewed told us that emergency rooms and mental health areas experience high levels of security incidents, requiring additional security measures in these areas.

VA specifies various physical security requirements for its medical centers. These include physical access control systems, security cameras, silent alarm distress signaling, and perimeter fencing. Furthermore, each VHA facility has its own police department to help deter, detect, defend against, and respond to security threats. See appendix II for more information regarding the roles and responsibilities of VA police departments. See figure 1 for a depiction of a medical center that consists of a campus and a variety of buildings and examples of the physical security elements deployed.

[7]Setback refers to the distance between a structure requiring protection and another building, the curb, a vehicle, or another object.

[8]VHA medical centers provide a wide range of services including traditional hospital-based services such as surgery, critical care, mental health, orthopedics, pharmacy, radiology, and physical therapy. In addition, VHA facilities may offer additional medical and surgical specialty services and may have buildings for research, warehousing, or administration services.

Figure 1: Examples of Physical Security Elements at Veterans Affairs' (VA) Medical Center Campus

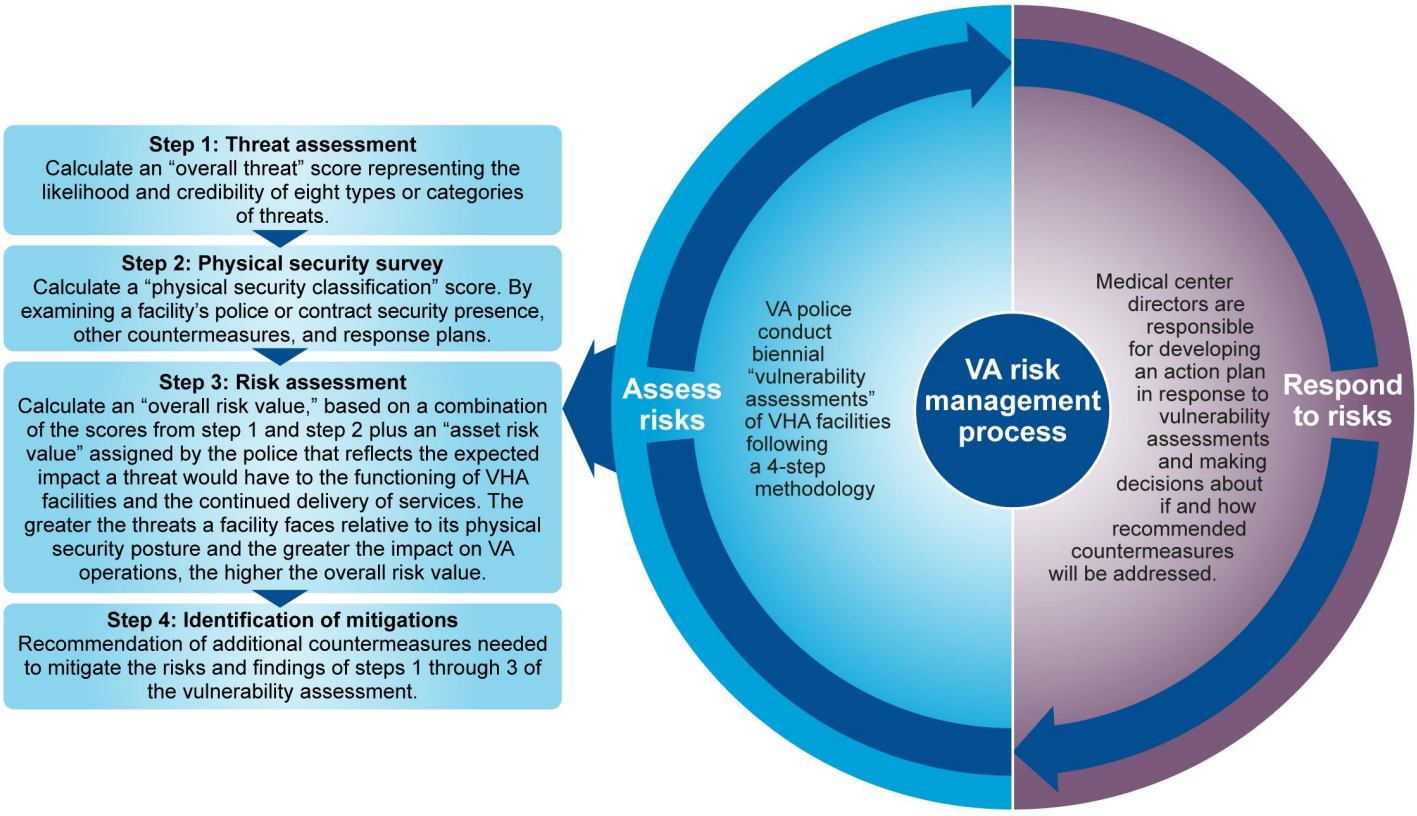


Source: GAO. | GAO-18-201

To determine the specific countermeasures needed at each facility, VA has a two-part risk management process that begins with VA police assessing a facility's security risk(s) by conducting "vulnerability assessments" biennially[9] (see fig. 2). VA police at each of VHA's medical centers report the findings, including recommended countermeasures, to medical center directors. These directors are responsible for developing an action plan in response to the assessments and making decisions about if and how recommended countermeasures will be addressed.

[9]VA police chiefs are responsible for ensuring that vulnerability assessments are performed for facilities under their jurisdiction. They may delegate this duty to officers or physical security specialists within their units.

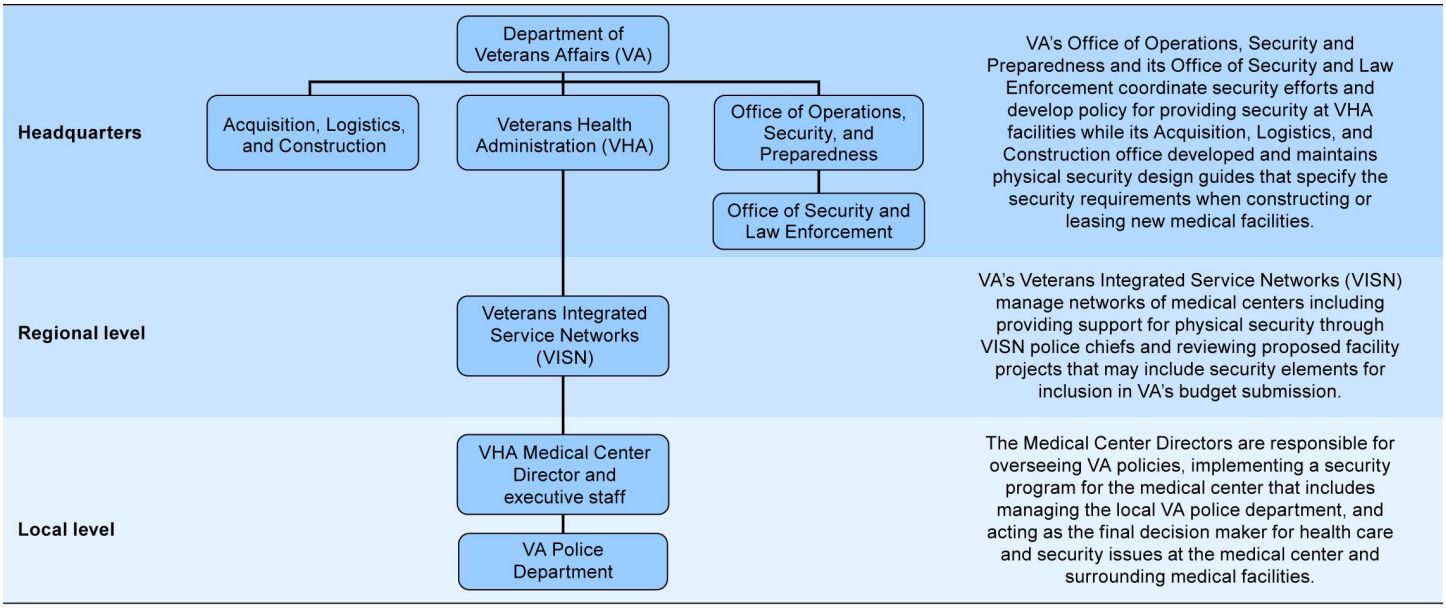
Figure 2: Veterans Affairs' (VA) Risk Management Process and Four-Step Vulnerability Assessment Methodology



Source: GAO analysis of VA policy. | GAO-18-201

Across VA, numerous entities at the headquarters, regional, and local level have some role in carrying out physical security responsibilities. Figure 3 provides an overview of VA components with physical security roles and responsibilities at VHA facilities.

Figure 3: Veterans Affairs' (VA) Components That Have Physical Security Roles and Responsibilities



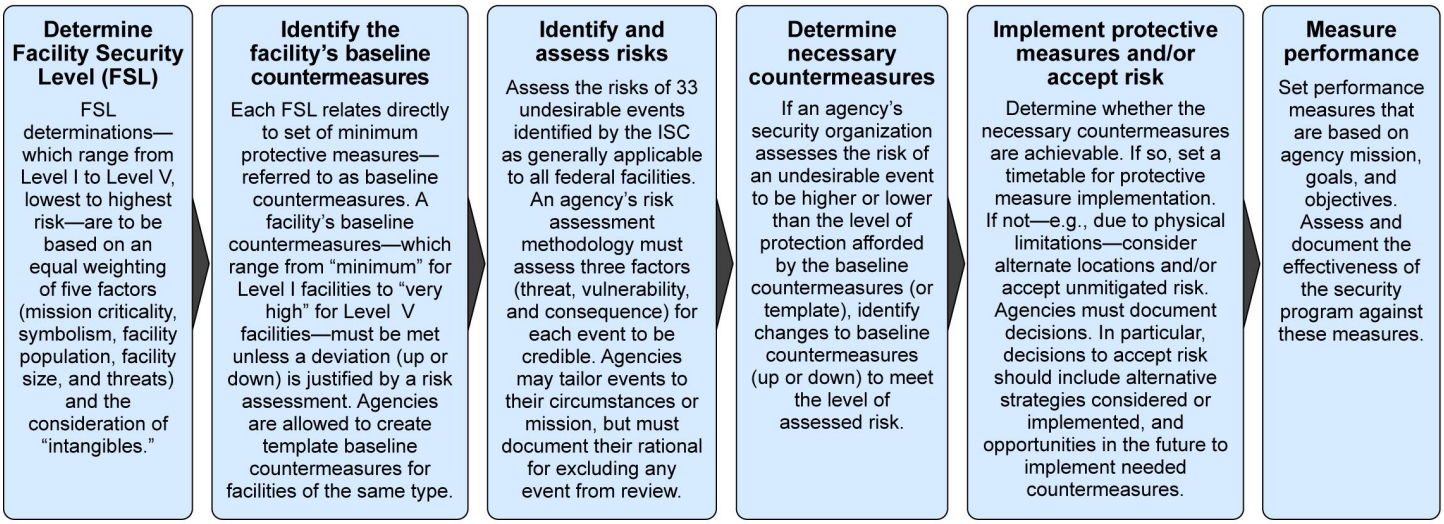
Source: GAO analysis of U.S. Department of Veterans Affairs (VA) information. | GAO-18-201

At the headquarters level, VA's Office of Security and Law Enforcement (OSLE), located within VA's Office of Operations, Security, and Preparedness, develops policies and standards for assessing physical security risks and providing physical security for facilities under VA's custody and control, including VHA facilities used for providing healthcare services to veterans. VA organizes its system of care into regional networks called Veterans Integrated Service Networks (VISN). Each VISN is responsible for managing and overseeing medical centers within a defined geographic area. However, the primary operational responsibility for VA's physical security program is at the medical centers themselves, where the medical center directors at each of VHA's 170 medical centers are responsible for implementing OSLE's policies and standards and overseeing VHA police activities. Police at each facility conduct the key activities involved in this program, including conducting risk assessments and identifying needed countermeasures. Beyond risk assessment, VA police have additional responsibilities for protecting the safety of medical centers. For information about their additional responsibilities and oversight of their operations, see appendix II.

The ISC was established via Executive Order 12977 in 1995 to enhance security at federal facilities. Its mission is to develop standards and best

practices.[10] ISC's Risk Management Process for Federal Facilities, among other things, includes standards for agencies' facility risk assessment methodologies. This process can help agencies effectively prioritize efforts to protect their facilities. ISC's process consists of six steps designed to help agencies identify the appropriate protective measures for their facilities, and to ensure their effectiveness. (see fig 4.)

Figure 4: The Interagency Security Committee's (ISC) Risk Management Process



Source: GAO analysis of Interagency Security Committee information. | GAO-18-201

ISC's Risk Management Process is applicable to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities, including special-use facilities. Agencies may customize their implementation of elements of ISC's standards, such as the countermeasures they determine are appropriate for their facilities or situations. Changes to these elements are to be made as a result of a risk-based analytical process. In December 2016, ISC issued its Agency and Facility Compliance Benchmarks to provide guidance to departments and agencies for ensuring compliance with ISC's standards.

[10]The ISC is housed within the Department of Homeland Security, and includes a membership of senior level executives from 60 federal agencies and departments, including VA. Executive Order 12977, Section 5(a)(2), 60 Fed. Reg. 54411 (Oct. 19, 1995), as amended by Executive Order 13286, 68 Fed. Reg. 10619 (Mar. 5, 2003).

VA's Risk Management Process Partially Reflects the ISC's Standard

VA's risk management process does not fully reflect the standards established by ISC shown in figure 4.[11] Although structured differently, we found that VA's process includes some elements of ISC's process but is missing other elements, gaps that could result in risks' not being fully assessed and appropriate countermeasures not being identified. See figure 5.

Figure 5: VA's Risk Management Process Compared to the Interagency Security Committee's (ISC) Risk Management Process

Interagency Security Committee (ISC) Risk Management Process Standard[a]	Department of Veterans Affairs (VA) Risk Management Process	
	☑ Reflects ISC standard	☐ Does not reflect ISC standard
Determine facility security level	VA police are to calculate and assign scores called "overall risk values" that represent a facility's level of risk.	VA's methodology for calculating overall risk values does not equally weigh factors nor does it include all factors specified by the ISC.
Identify the facility's baseline countermeasures	VA has created templates of baseline countermeasures for different types of areas or facilities (e.g. medical center pharmacy).[b]	–
Identify and assess risk	VA police are to assess threats, vulnerabilities, and consequences in 8 threat categories.	VA lacks documentation on how its 8 threat categories relate to ISC's 33 undesirable events and why certain undesirable events appear to be excluded.
Determine necessary countermeasures	VA police are to conduct biennial assessments and recommend countermeasures.	VA policy does not require recommended countermeasures be related to the baselines established in its templates.
Implement protective measures and/or accept risk	Local medical center directors are to review information from vulnerability assessments and determine if and how to implement recommended countermeasures.	VA does not have policies requiring officials to document the acceptance of risk, including the rationale for rejected or deferred countermeasures, proposed alternative mitigations, and future planning.
Measure performance	–	VA does not have policies or performance measures in place for assessing the effectiveness of its security program.

Source: GAO analysis of U.S. Department of Veterans Affairs (VA) information. | GAO-18-201

[11]Similarly, in 2013, we reported that VA did not use ISC standards for all of its facilities. GAO, *Facility Security: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies*, GAO-13-222 (Washington: D. C.: Jan. 24, 2013). In 2014, we also reported that VA's risk assessment methodology did not align with the ISC standards. GAO, *Additional Actions Needed to Help Agencies Comply With Risk Assessment Methodology Standards,* GAO-14-86 (Washington: D. C.: March 5, 2014). We recommended that the ISC conduct additional outreach and assess agency compliance with its standards. ISC has completed some outreach and is in the process of formulating a process for validating agency compliance with its standards

[a]ISC, The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (November 2016).

[b]We did not review VA's process for developing these templates.

Determine facility security level: ISC's standard requires that facility security levels (I-V) are to be based on an equal weighting of five factors (mission criticality, symbolism, facility population, facility size, and threats) and the consideration of "intangibles." According to the ISC, each of these factors is important to quantifying a facility's attractiveness as a target for adversarial acts and the severity of consequences should such an act occur.

VA policy calls for three of the factors to be used in determining a facility's risk level, which partially reflects the ISC Standard. VA policy indicates that VA police are to identify an "asset risk value" that reflects the expected effect a threat would have to the functioning of VHA facilities and the continued delivery of services. This score is used to calculate an "overall risk value." The greater the threat a facility faces relative to its physical security posture and the greater the impact on VA operations, the higher the overall risk value. The determination of the overall risk value reflects the ISC's prescribed use of facility security levels to identify a facility's level of risk.

VA's policy does not articulate that factors used to determine the overall risk value be equally weighted, nor does it include facility population and facility size as factors. As a result, VA may not be considering all the relevant risk factors that make a facility a more or less desirable target for threats.

Identify the facility's baseline countermeasures: The ISC Standard calls for baseline countermeasures to vary based on facility's risk level. For example, depending on a facility's security level and the type of undesirable threat posed, the use of X-ray or magnetometers may be required to screen visitors. Alternatively, agencies are allowed to create templates by facility type. That is, an agency can identify the specific risks posed to particular facility types and customize different sets of countermeasures that can serve as the baseline for those facility types.

VA has created templates based on facility types rather than varying its baseline countermeasures relative to a facility's risk level, which is

permissible under the ISC Standard.[12] These templates outline the specific minimum countermeasures for different types of facilities or components of VHA facilities such as medical center pharmacies.[13] VA's minimum requirements for countermeasures in their facilities were designed to meet the needs of the medical center environment and clientele.

Identify and assess risk: ISC has established 33 specific undesirable events that agencies are to use when assessing risks to facilities. Additionally, the ISC requires that an agency's risk assessment methodology consider three factors—threat, vulnerability, and consequence—in examining these events in order to be credible. [14] Agencies may customize the threats they assess to their specific situations, after having considered the 33 undesirable events.[15] According to ISC officials, agencies are expected to periodically review their list of undesirable events as updates to the standards occur and document determinations and justifications for excluding any undesirable event.

VA has identified 8 categories of threats that VA police are to review as part of vulnerability assessments, which includes consideration for threat, vulnerability, and consequence. These threat categories are: 1) assault, 2) physical threats of violence, 3) illegal weapons, 4) suicidal behavior, 5) theft/vandalism, 6) explosive devices, 7) mail-borne hazards, and 8) protection of hazardous materials and narcotics. This listing reflects the ISC Standard that agencies examine risks from undesirable events.

[12]These minimum requirements are outlined in Appendix B of VA Handbook 0730/4, which is directed to VA police. These requirements are applicable to existing buildings. VA has also developed physical-security design criteria that are applicable to new construction and major renovations. For the purposes of our report we focused on the requirements for existing buildings.

[13]We did not review VA's process for developing these templates.

[14]Threats are the intentions and capabilities of adversaries to initiate undesirable events; consequences are the level, duration, and nature of losses resulting from undesirable events; vulnerabilities are weaknesses in the design or operation of a facility that adversaries can exploit. Undesirable events represent the "reasonable worst case scenario" for each threat. Risk assessment methodologies involve assigning ratings to each of the three factors and combining these ratings to produce an overall measurement of risk for each identified undesirable event.

[15]According to ISC officials, the term "consider" means that as a starting point or baseline, an agency's methodology must include all of the undesirable events listed in the ISC Standard.

However, VA cannot demonstrate how its categories relate to ISC's 33 undesirable events. According to VA officials, VA originally selected its threat categories in 2001 and updated them in 2009 to the current 8 categories. They told us that officials at the time considered the ISC's full list of undesirable events and that these eight threat categories were and remain the most prevalent in the health care's operating environment that represents the majority of VHA facilities. However, officials could not provide documentation of how their eight categories related to ISC's defined undesirable events and why certain undesirable events appear to be included and others excluded within VA's policies pertaining to risk management. By not reviewing all the undesirable events identified by the ISC, VA may be overlooking some potential threats present at its facilities.

Determine necessary countermeasures: ISC calls for agencies to determine if their baseline countermeasures or templates address a facility's established risk level following an assessment. ISC has also clarified that its standards allow for countermeasures to be customized to specific facilities and situations. For instance, if the risks from undesirable events at a specific facility are found to be higher or lower than the level of protection afforded by the baseline set of countermeasures, the baseline countermeasures can be changed (up or down) to meet the level of assessed risk.

VA policy calls for police at each of VHA's medical centers to conduct vulnerability assessments biennially. As a part of these assessments, VA police are to recommend countermeasures that represent the best value in terms of providing protection against multiple threats given the existing level of defense or security equipment. This procedure reflects the ISC Standard that necessary countermeasures be identified at the facility level by an agency's security organization.

However, VA policy does not require recommended countermeasures to be related to the baselines established in the templates. This policy is inconsistent with the ISC Standard, which calls for countermeasures to be increased or decreased from the baseline to meet the level of assessed risk. This policy could leave staff, patients, and visitors, as well as property vulnerable to unmitigated risks.

Implement countermeasures or accept unmitigated risk: The ISC Standard requires agencies to document decisions, in particular, any decision to reject or defer implementation of countermeasures due to cost (or other factors). The ISC Standard also requires agencies to document

the acceptance of risk in these instances and outline alternative strategies considered or implemented, and opportunities in the future to implement needed countermeasures. The ISC Standard notes, in particular, that risks accepted at the facility level may have a bearing on agency-wide risk management efforts and therefore documentation of risk acceptance shall be provided to the headquarters security office.

As previously discussed, medical center directors are to determine if and how to implement recommended countermeasures. This reflects the ISC Standard that information from assessments be forwarded to and used by decision makers. However, VA policy does not require the documentation of risk acceptance. That is, VA has no policy requiring its officials to document the rationale for rejected or deferred countermeasures, proposed alternative mitigations, and future planning.[16] Without such a requirement, OSLE does not have full knowledge of the extent of risk acceptance that has occurred or what alternative countermeasures have been pursued.

Measure performance: According to the ISC Standard, agencies are to assess and document the effectiveness of their security program through performance measurement and testing. Measures should be based on agency mission goals and objectives. As examples of performance measures, the ISC Standard suggests that agencies could track the number of countermeasures in use or the percentage of facility assessments completed. Moreover, the ISC Standard states that agency-level leadership must communicate its priority and commitment to performance measurement and ensure that the physical security performance measures enhance accountability, prioritize security needs, and justify investment decisions to maximize available resources.

VA lacks documented policies or performance measures in place for assessing the effectiveness of its security program, which does not reflect the ISC Standard. VA policy outlines that local medical-facility directors at VHA facilities shall ensure that law enforcement activities (such as vulnerability assessments) are conducted in a legally and technically correct manner, but provides no guidance to ensure uniform measures

[16]VA policy includes some requirements for documenting decision-making regarding deficiencies identified in physical security surveys, which are distinct and separate from vulnerability assessments. Specifically, if individual VHA facilities cannot meet the minimum countermeasures (e.g., because of physical limitations), VA policy indicates that officials must request a waiver and/or approval for alternative mitigations from VA's OSLE.

and processes are being used to assess the performance of security programs. Without a policy that establishes uniform performance measures, VA cannot evaluate the effectiveness of physical security programs being locally implemented across its facilities.

According to VA officials, VA's risk management process was developed before the ISC's standard for risk management processes was originally issued in 2013. VA officials we spoke with said as a member of ISC they utilize it as a forum for exchanging ideas on best practices and interpreting the standards but it is then up to each agency to determine how best to apply ISC standards.[17] VA officials said that they are currently reexamining their policies but have not reached out to the ISC for assistance. ISC officials told us they are available to act as resource for any agency requesting aid in developing or reviewing risk management processes.

VA cannot assure that the differences between its process and the ISC Standard are inconsequential to how it identifies and manages risk at local facilities and across its real property portfolio. According to the ISC Standard, not using an appropriate risk-management process can result in facilities that may either have (1) less protection than needed resulting in inadequate security or (2) more protection than needed resulting in an unnecessary use of resources. This situation might reduce the availability of resources that could be applied elsewhere. For example, although all VHA medical centers have the same mission, variations in location and physical configuration of a facility may create unique risks or risks that are relatively higher or lower in some cases than at other VHA facilities with the same mission.

[17]In its technical comment to this report, VA pointed out that under federal regulations (41 C.F.R. § 102-81.25), certain types of special-use facilities, such as hospitals, are exempt from ISC design criteria standards. For the purpose of our report, we reviewed VA policies pertinent to its risk management process and its risk assessment methodology and compared the policies to ISC's risk management standards. As such, ISC's design criteria standards did not apply to our assessment and were outside the scope of our review. As we previously discuss in the report, ISC's Risk Management Process is applicable to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities, including special-use facilities.

VA Does Not Assess the Effectiveness of Its Risk Management Process

Agencies are expected to manage the effectiveness of program operations in achieving their missions. A range of federal standards and guidance assist agencies improve the accountability and effectiveness of their programs by helping agencies adapt to shifting environments, evolving demands, changing risks, and new priorities. For example, in July 2016, OMB updated guidance to establish management's responsibilities for enterprise risk management (ERM). ERM is intended to yield an "enterprise-wide," strategically aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.[18] More specifically, the guidance discusses both internal control and ERM and how these fit help together to manage agency risks. Additionally, Standards for Internal Control in the Federal Government describes internal control as a process put in place by an entity's oversight body, management, and other personnel, a process that provides reasonable assurance that objectives related to operations, compliance, and reporting will be achieved, and that serves as the first line of defense in safeguarding assets.[19] Elements within these standards include:

- holding people accountable for their responsibilities,
- having effective operations that produce intended results in a manner that minimizes the waste of resources, and
- using quality information to achieve objectives.

However, according to OSLE officials, OSLE does not assess program effectiveness, Instead, officials said that OSLE's role in overseeing VHA's risk management process is limited to reviewing the activities of each

[18]OMB, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123, (July 15, 2016).

[19]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: September 2014).

VHA medical center's police department's activities.[20] Specifically, as it relates to the risk assessment process discussed earlier, the OSLE review focuses on whether (1) vulnerability assessments are completed within the required time frame (at least every 2 years); (2) annual physical security surveys that are used to inform the vulnerability assessments are completed and documented, and (3) intruder detection tests are completed. The OSLE inspectors may also spot-check specific areas to determine whether physical security measures that are in place meet VA's standards. The areas checked are at their discretion and not identified in policy. Findings from these inspections, including any deficiencies identified in physical security, are reported to the medical center director for action.

According to OSLE officials, they do not have any authority to ensure deficiencies are corrected and thus generally do not follow up on the status of their findings prior to the next inspection. Although the results of these inspections are stored by OSLE, we did not find that it uses them to identify trends in security deficiencies or track medical centers' risk levels.

OSLE does not assess the medical center's compliance with VA's overall risk management process, the extent to which recommended security measures have been implemented, or decisions not to implement security recommendations. Furthermore, OSLE does not collect data that would allow it to know what security deficiencies have been identified across all VHA facilities and the status of recommended countermeasures. Because VHA lacks an oversight strategy that includes these elements, it cannot begin to assess the effectiveness of security at its facilities.

The lack of a system-wide oversight strategy is particularly troublesome given the authority and autonomy of medical center directors to determine the appropriate physical security measures needed for their facilities. At the nine medical centers, we found differences in how they implemented the risk management requirements and countermeasures and in how they collected security related data. Without a strategy for system-wide oversight, VA cannot ensure that local physical security-decisions are

[20]Police department programs are inspected every 2 years. The responsibility for conducting these inspections is shared by VA's Office of Security and Law Enforcement and the VISN Police Chief, with each conducting the inspections once every 4 years. OSLE inspectors use a checklist to review specific aspects of several areas including personnel and training; administration; operations; equipment, weapons and weapons control; physical security, and outcomes and customer satisfaction.

based on actual risk, are appropriate to protect the facility, and are effective, or whether the variations or the security impact of them are important.

Implementing VA's risk management requirements: A key element of internal controls is having a process in place to hold people accountable and ensure that the agencies' policies are being implemented as intended. While OSLE's inspections assess whether the vulnerability assessments were completed, we found that they did not assess the quality of those assessments or whether they aligned with VA's policy requirements. Specifically, we found differences in how the assessments were done at the nine medical centers we reviewed and that some were not consistently reviewing the full range of threats required by VA policy. For example, none of the vulnerability assessments we reviewed included documentation that all eight of VA's threat categories were reviewed, and at three locations, no threat categories were documented as reviewed in the assessments. Additionally, in some instances, VA police assessed different threat categories than the required 8 categories. OSLE officials told us that local VHA police have the discretion to review any threats they perceive relevant to their facility; however, they reported that this should be done in addition to the eight threat categories identified in VA guidance. In a decentralized environment such as VA's, there may be greater risk that VA police will inconsistently apply VA's risk management process. Furthermore, as discussed earlier, VA has not established performance measures, in accordance with ISC standards, for its risk management process. This, according to the ISC, would help to ensure accountability, prioritize security needs, and justify investment decisions to maximize available resources.

Implementing countermeasures: Internal controls guidance speaks to having effective operations that produce intended results in a manner that minimizes the waste of resources. ERM also speaks to the effective and efficient use of resources. We found wide variation in the progress made in implementing countermeasures across the nine locations we reviewed. This variation happens, in part, because of competing priorities and lack of dedicated physical- security budgets. As a result, medical center directors make localized decisions about where they spend their resources. The police force is responsible for identifying appropriate countermeasures, but it is then up to the medical center directors and the managers in the areas for which deficiencies have been identified to implement the corrective actions. All of the medical center directors we interviewed reported weighing decisions to fund infrastructure deficiencies affecting healthcare delivery versus funding physical security projects. For

example, one acting director told us that the center needs to repair a leaking roof in its hospice care unit. The director told us that this project, which uses funding from the same pool of money as physical security projects, will be prioritized because it directly impacts the quality of patient care.

Officials at the sites we reviewed described varying levels of commitment from medical center directors to prioritize physical security infrastructure projects. Officials at one site said that they currently have difficulty getting the resources they request to implement security countermeasures, but that the same had not been the case at previous medical centers where they worked. Specifically, one official noted that it can be difficult to convince a medical center director to fund security measures designed to protect the site from situations that have not yet occurred, such as countermeasures to improve perimeter security or increase standoff distance for critical areas, which are important parts of prevention for active-shooter type scenarios.

One of the key countermeasures medical centers use for physical security is the police force. We noted variations in police staffing at the nine locations we studied. VA policy sets a minimum level for the number of VA police officers who must be on patrol at any given time if certain conditions are met. Some local VHA officials we spoke with said they need to staff above this level because following the minimum staffing level can be problematic when officers are needed to respond to multiple incidents at the same time, such as escorting one patient and responding to a disruptive patient in a different wing of the hospital, officials stated. Officials noted that incidents can be the driving factor for changes. One site we reviewed increased their police presence in the emergency room, in response to a stabbing incident that occurred there.

The critical role that police play at these medical centers can be adversely affected, however, because of challenges related to recruiting and retaining law enforcement personnel. All sites we reviewed reported hiring vacancies in their departments, and multiple sites discussed challenges in maintaining any police at the recommended level at their facilities, hindering the ability of the police to respond to multiple incidents.[21] As

[21]VA reported it has approved about 4,700 full-time employee police positions, but nearly 700 of these positions remain vacant.

further described in appendix II, each VHA medical center police force is managed locally, under the control of the medical center director.

We also found varying levels of security provided by VA medical centers for their community based outpatient clinics. VA policy does not require a permanent security presence at the community-based outpatient clinics, and medical centers may rely on local police to respond to security incidents. However, some sites we reviewed use contract guards to provide a security presence at outpatient clinic locations, and one site reported completing an effort to staff VA police officers at each of the outpatient clinics under the medical center director's authority. In the absence of system-wide oversight strategy, VA does not know if these variations in countermeasures are resulting in different levels of security, which may leave some facilities at risk and not be the most strategic use of resources at other facilities.

Tracking security deficiencies: The availability of reliable data is essential for assessing the effectiveness of policies and programs and for allowing managers to make sound decisions. In the absence of a VHA-wide strategy and guidance about how to collect data or track deficiencies, individual sites have established their own processes for tracking the status of identified security deficiencies. For example, one of the medical centers in our review reported 15 deficiencies resulting from its assessment, whereas another medical center reported over 540 deficiencies. In reviewing the data further, we found that the numbers may be misleading as to the extent of security concerns, because of the different ways in which the findings were reported. For example, in reporting the results of inspections of information telecommunication and data closets, one location identified a recurring deficiency as one issue, where another location identified a similar deficiency in each closet they inspected resulting in over 200 identified deficiencies. A system-wide oversight strategy could help VA identify what information is needed to assess the effectiveness of its security programs and the impact of varying practices at its facilities.

In the past, VA collected system wide information and tracked physical security across medical centers. When VA first started conducting vulnerability assessments in 2010, the assessments were done by a central team directed by OSLE, and the findings were tracked in a central database. In addition, a work group tracked how facilities were meeting VA's standards and requirements and which countermeasures were getting prioritized and implemented. However, VA officials told us that this database crashed and that the information is no longer accessible.

Moreover, the central team was dissolved, and medical center directors became fully responsible for ensuring that vulnerability assessments were conducted. The collection or assessment of data also became the responsibility of local medical centers.

Although OSLE has no current plans to re-establish a database, in 2015 the Acting Deputy Under Secretary for Health for Operations Management identified a need for information about the level of security at its facilities. He has directed VISN management to identify gaps between its facilities and VA's 2015 physical-security design standards.[22] This effort is separate from VA's risk management process but would be expected to identify some of the same security deficiencies. VISNS are expected to use these results to develop and prioritize projects to bring facilities in line with the current VA physical security standards.

Conclusions

VA faces the challenge of providing secure, open, and welcoming medical facilities while providing medical care for nearly 9-million veterans annually. Having a process that incorporates ISC standards is critical to VA and ensuring that it is positioning itself to appropriately protect its facilities. However, until VA reviews its policies against the ISC standards to explore areas where it differs from these standards, it will not be able to ensure that its approach to risk management will yield and has yielded the appropriate security posture relative to the different risks faced by its diverse set of facilities. While not currently required, collaboration with the ISC would be helpful for the VA as it reexamines its risk management process. Additionally, the decentralized nature of VA's organizational structure can help VHA tailor its programs to local situations. But without a system-wide oversight process, VA cannot assess the overall performance of its security program and whether medical centers are adequately protected. Thus, it may be missing opportunities to leverage resources nationally, or make informed, proactive policy decisions.

[22]In 2015, VA published design and construction standards to provide for the physical security of new buildings, additions, and major alterations of VA owned and operated facilities.

Recommendations for Executive Action

We are making the following two recommendations to VA:

The Secretary of VA should, in collaboration with ISC, review and revise VA's risk management policies for VHA facilities to ensure VA incorporates ISC standards, as appropriate. (Recommendation 1)

The Secretary of VA should develop an oversight strategy that allows VA to assess the effectiveness of risk management programs at VHA facilities system-wide. (Recommendation 2)

Agency Comments

We provided a draft of this report to the Department of Veterans Affairs (VA) and Department of Homeland Security (DHS) for comment. In written comments, which are reproduced in appendix III, VA agreed with our conclusions and concurred with our recommendations. In its comments, VA stated that it is in the process of updating its vulnerability assessment program and will work with the ISC to ensure VA is in compliance with applicable standards. VA also stated that it will work with the ISC as VA updates its risk management process to ensure it reflects the applicable standards established by the ISC. VA also intends to evaluate its current roles and responsibilities for assessing internal controls for risk management. VA estimates that it will complete these actions by January 2019. VA also provided a technical comment, which we have clarified in the report. DHS provided only technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretary of the Department of Veterans Affairs; the Secretary of the Department of Homeland Security; and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov. If you or your staff have any questions about this report, please contact me at (202) 512-2834 or rectanusl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,

Lori Rectanus
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our report were to assess (1) the extent that VA's policies for physical-security risk management reflect elements of federally established risk management standards and (2) VA's oversight of risk management of physical security at VHA facilities. To help inform our research, we reviewed reports and documentation on physical security. For example, we reviewed prior reports from GAO on the security of federal government facilities and effective program management, as well as documentation from the Department of Homeland Security's Interagency Security Committee (ISC), including physical security standards it has developed by the ISC. Our review focused on security at medical facilities under the custody control of VHA.

To determine how VA policies for physical security risk management reflect key elements of federally established risk management standards, we assessed how VA's methodologies reflect ISC's risk management standards. This included reviewing the Risk Management Process for Federal Facilities (the ISC Standard) for assessing physical security and providing recommended countermeasures at federal facilities.[1] We obtained and analyzed VA's facility-security policies and procedures for a risk management methodology. According to the ISC Standard, agencies' risk management methodologies should

- determine facility security level (FSL);
- identify facility's baseline countermeasure;
- identify and assess risk;
- determine necessary countermeasures;
- implement protective measures and/or accept risk; and
- measure performance

To assess VA's oversight of risk management of physical security at VHA facilities, we identified and examined oversight and management mechanisms at the national, regional, and local levels, including reporting

[1]ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D. C.: November 2016).

mechanisms that prioritize or track facility risks or the implementation of countermeasures at VHA facilities. We also reviewed Standards for Internal Control in the Federal Government because internal controls play a significant role in helping agencies achieve their mission related responsibilities using proper oversight mechanisms.[2] To help determine if VA has established an environment in which it can ensure it is achieving its objectives, we reviewed agency documentation, such as vulnerability reports, police inspections, and the tracking reports related to security countermeasure recommendations at a non-generalizable sample of 9 VA medical centers. At these locations, we also conducted semi-structured interviews with facility management, VA police, and union representatives to identify the officials' approach to physical security. Our findings from our review of the selected medical centers are not generalizable to all VHA facilities, but provide insight into and illustrative examples about risk-management and oversight methodologies at selected facilities.

We selected these sites based on a mix of criteria that included: (1) geographic location, including medical centers in various Veteran Integrated Service Networks (VISN), and in cities of different sizes; (2) patient volume, including medical centers with a mix of different levels of patient population; (3) reported security incidents, including locations with high and low levels of reported security incidents ; and (4) patient to incident ratio, including medical centers with high and low ratios of incidents per patient, among other considerations. Based on the selection criteria listed above, the team selected the following nine medical center locations for our review:

1. Bedford, MA
2. Houston, TX
3. Greater Los Angeles
4. Bay Pines, FL
5. Sheridan, WY
6. Washington, D.C.
7. Puget Sound, WA
8. Orlando, FL

[2]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D. C.: September 2014).

9. Louisville, KY

Considering the extent to which VA uses its police force in its risk management approach, we also reviewed the lines of authority and oversight for VA police personnel. For example, we identified VA's police-reporting structures and data-collecting efforts.

We conducted this performance audit from September 2016 to January 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Overview of VA Police Departments' Roles and Responsibilities

The Department of Veterans Affairs (VA) police consist of over 4,000 uniformed police officers in 153 police units across the nation. Each VHA medical center has, in effect, its own police force.[1]

Key Activities

Aside from VA's role in assessing physical security risks, VA police's day-to-day role at VHA medical centers largely revolves around their law enforcement functions. Specifically, police officers patrol medical center campuses in an effort to deter, detect, defend, and respond to threats to patients and staff. Officers can make arrests for violations of federal law, can confiscate drugs, alcohol or other contraband, and can conduct investigations and collect basic evidence to the extent necessary to determine whether a crime has been committed.[2] In addition, VA police officers might respond to incidents involving disruptive patient behavior—a continual concern for staff at VHA facilities, according to officials from the sites we spoke with. Staff can alert VA police to such incidents through means such as duress alarm systems at their facilities, and at some locations we spoke with, police respond as part of multi-disciplinary teams that try to de-escalate incidents involving disruptive patients. For example, police can be on the Disruptive Behavior Committees at their facilities. These multi-disciplinary committees review incidents involving

[1]VA Police were established in 1991 under Chapter 9 of Title 38 and given the authority to enforce federal laws on Department of Veterans Affairs' property. Provisions in Title 38 USC, Sections 902 and 904 give authority to the VA Secretary to furnish VA police officers with such weapons as the Secretary determines to be necessary and appropriate to ensure the maintenance of law and order and the protection of persons and property on Department property. Following a pilot program to arm VA police in 1998, VA issued directive 0720 in January of 2000, providing policies to establish a program to provide firearms to VA police officers for carry and use on duty. See 38 C.F.R. § 1.218(c) and 38 U.S.C. § 902(b). VHA medical centers that are part of a Health Care System may be supported by one VA police department. For example, the VA police for the Puget Sound Health Care System support two medical centers: the Seattle Division and American Lakes Division.

[2]As specified in VA Handbook 0730, Title 38 CFR § 1.218, and Titles 18 and 21 U.S.C.

disruptive patients and can suggest mitigations for future incidents including placing a "flag" on a patient's record. These flags alert staff to prior concerns with a patient's behavior and may include instructions for preventative measures such as a requiring the patient to check in with VA police when arriving on campus or requiring the patient to have a police escort while at the facility.

VA police at some sites included in our review described challenges officers face when responding to incidents. For example, according to VA police officials, not all incidents involving disruptive patients constitute a violation of the law, limiting the ability of a police officer to intervene. Police officials spoke about trying to de-escalate situations first, before making arrests or physically intervening in an altercation. Furthermore, VA police officers are limited in their authority to engage in certain actions such as pursuing non-federal offenses, investigating crimes off-campus, and carrying service weapons off campus, officials told us. In addition, some VA police we spoke with stated that the Assistant U.S. Attorney's office is reluctant to prosecute veterans, so the VA police do not have much leeway or leverage in detaining, arresting or pressing charges against patients or visitors. For example, according to VA police officials from one site we spoke with, the Assistant U.S. Attorney declined to prosecute a stabbing incident. As a result the police had to work with the local police to recharge the case and go through the state court for prosecution.

As a part of the policing role, police have various reporting responsibilities. For example, police officers are expected to report their daily operational activity into a computerized database called the VA Police System that: (1) documents all criminal activity at the medical centers, (2) records daily incident reporting at each facility in a 24-hour period, and (3) lists all individuals who come into contact with VA police.[3] VA police chiefs at each location use this data to generate a localized Unified Crime Report (UCR) for each campus. Each police chief maintains his or her own UCR, which can include all incidents reported by officers, from petty theft to homicide. VA police are to conduct predictive analysis of crime patterns and adjust patrols or investigative activities accordingly.

[3]VA is in the process of moving from its current Veterans Affairs Police System (VAPS) database to a new system called Report Exec.

In addition to recording all activities into the database, VA police are required to report certain incidents (including incidents that are likely to result in national media or congressional attention), to the VA's Integrated Operations Center through a Serious Incident Report.[4] Police officers are required to report serious incidents as soon as possible, but no later than 2 hours after awareness of the incident. Reportable incidents include, among others, sexual or aggravated assaults and VA police-involved shootings.[5] The Integrated Operations Center staff provides reports and real-time information on these incidents to the Secretary and the VA administrators for their awareness; however, the staffers do not conduct their own investigations into incidents. Officials from the Office of Security and Law Enforcement told us that they have started pulling together internal, monthly rollups of law-enforcement-related serious incident reports. These reports are provided to the VA police chiefs to inform them of serious incidents and provide situational awareness on law enforcement and criminal activity happening at VHA medical centers across the nation. These reports contain law-enforcement sensitive information and are intended for internal VA police use for crime analysis specific to VA law enforcement matters affecting VA campuses and are not to be released to the public or individuals or organizations outside law enforcement.

Police Oversight and Management

The Office of Security and Law Enforcement (OSLE) develops and issues policies and procedures for physical security, law enforcement, and training activities for VA police.[6] In addition, OSLE and VISN police chiefs share responsibility for the police inspection program described in this

[4]See VA Directive 0321, issued in 2012.

[5]Serious Incidents are defined by nine criteria listed within VA Directive 0321 and include: 1) public information regarding the arrest of a VA Employee; 2) major disruption to the normal operations of a VA facility; 3) deaths on VA property due to suspected homicide, suicide, accidents, and/or suspicious deaths; 4) VA Police-involved shootings; 5) Activation of Occupant Emergency Plans, Facility Disaster Plans and/or Continuity of Operations Plans; 6) loss or compromise of VA sensitive data, including classified information; 7) theft or loss of VA-controlled firearms or hazardous material, or other major theft or loss; 8) terrorist event or credible threat that affects VA facilities or operations; 9) Incidents on VA property that result in serious illness or bodily injury to include sexual assault, aggravated assault and child abuse.

[6]OSLE issues policies and procedures to the local VA police departments through its VA Handbook 0730 and subsequent updates.

report. OSLE does not provide any sort of centralized command over police chiefs or officers, however. This level of oversight and management of VHA police is done through the senior leadership at each local medical center. Police chiefs set the standard- operating procedures for their departments and report to an associate or assistant medical director, who provides daily supervision and approves their performance management appraisals. Medical center directors are ultimately responsible for the hiring of VA police officers and funding their training through VA's Law Enforcement Training Center.[7]

If allegations of police misconduct arise, the local VA police departments, and specifically the police chiefs, are responsible for investigating these claims. According to officials we spoke with, there are multiple methods police misconduct can be reported: directly through the medical center; to the VA Inspector General complaint hotline, or, in some instances, directly to OSLE within VA's headquarters. OSLE's Criminal Investigation Division will generally investigate criminal allegations and if appropriate will refer issues to the US Attorney for action. OSLE does not have supervisory authority over the VA police departments, and so any administrative actions must be taken by the local medical center officials.

[7]VA police are trained at its Law Enforcement Training Center at a cost of about $11,000 per officer. The training center is a subordinate organization under the Office of Security and Law Enforcement that operates as a franchise fund, and budget and staffing levels are based on revenue generated by reimbursable services provided by the center.

Appendix III: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

December 20, 2017

Ms. Lori Rectanus
Director
Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Rectanus:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***"VA FACILITY SECURITY: Policy Review and Improved Oversight Strategy Needed*** (GAO-18-201).

The enclosure provides general and technical comments, and sets forth the actions to be taken to address the GAO draft report recommendation.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Gina S. Farrisee
Deputy Chief of Staff

Enclosure

Department of Veterans Affairs (VA) Comments to
Government Accountability Office (GAO) Draft Report
"VA FACILITY SECURITY: Policy Review and Improved Oversight Strategy Needed
(GAO-18-201)

Recommendation 1. The Secretary of VA should, in collaboration with Interagency Security Committee (ISC), review and revise risk management policies for VHA facilities to ensure VA incorporates ISC standards, as appropriate.

VA Comment: Concur. The Department of Veterans Affairs (VA) is in the process of updating our vulnerability assessment program and will work with the Interagency Security Committee (ISC) as we update our process to ensure we are in compliance with applicable standards.

Representatives from VA's Office of Security and & Law Enforcement are scheduled to meet with the Program Director and staff members from the ISC to discuss the process of incorporating ISC standards with VA Handbook 0730/4 Physical Security Requirements.

As noted in the draft report, Veterans Health Administration (VHA) is responsible for physical security at its facilities and has issued polices and standards that the facility must follow when assessing physical security risk. Since August 11, 2000, VHA has implemented physical security policies and standards as reflected in VA Handbook 0730. Throughout the years, security risk has prompted continued updates to the handbook, rendering it a living document mandating the appropriate procedural changes in an effort to protect lives and property within VA's jurisdiction. These standards consist of a wide range of security countermeasures specific to VA's culture (medical center environment) clinical and environmental management operations. Target Completion Date: January 2019.

Recommendation 2. The Secretary of VA should develop an oversight strategy that allows VA to assess the effectiveness of risk management programs at the VHA facilities system wide.

VA Comment: Concur. VA will work with the ISC as we update our risk management process to ensure it reflects the standards established by ISC as applicable. In addition, we will evaluate the current roles and responsibilities for assessing our internal controls for risk management in order to improve our process. Target Completion Date: January 2019.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Lori Rectanus, (202) 512-2834, or rectanusl@gao.gov

Staff Acknowledgments

In addition to the individual named above, Maria Edelstein (Assistant Director); William Carpluk; Raymond Griffith; Geoffrey Hamilton; Joshua Ormond; Amy Rosewarne; Friendly Vang-Johnson; and Elizabeth Wood made key contributions to this report.

Appendix V: Accessible Data

Agency Comment Letter

Text of Appendix III: Comments from the Department of Veterans Affairs

Page 1

December 20, 2017

Ms. Lori Rectanus Director

Physical Infrastructure Issues

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Ms. Rectanus:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, "VA FACILITY SECURITY: Policy Review and Improved Oversight Strategy Needed (GAO-18-201).

The enclosure provides general and technical comments, and sets forth the actions to be taken to address the GAO draft report recommendation.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Gina S. Farrisee Deputy Chief of Staff

Enclosure

Page 2

Department of Veterans Affairs (VA) Comments to Government Accountability Office (GAO) Draft Report

"VA FACILITY SECURITY: Policy Review and Improved Oversight Strategy Needed"

(GAO-18-201)

Recommendation 1. The Secretary of VA should, in collaboration with Interagency Security Committee (ISC), review and revise risk management policies for VHA facilities to ensure VA incorporates ISC standards, as appropriate.

VA Comment: Concur. The Department of Veterans Affairs (VA) is in the process of updating our vulnerability assessment program and will work with the Interagency Security Committee (ISC) as we update our process to ensure we are in compliance with applicable standards.

Representatives from VA's Office of Security and & Law Enforcement are scheduled to meet with the Program Director and staff members from the ISC to discuss the process of incorporating ISC standards with VA Handbook 0730/4 Physical Security Requirements.

As noted in the draft report, Veterans Health Administration (VHA) is responsible for physical security at its facilities and has issued polices and standards that the facility must follow when assessing physical security risk. Since August 11, 2000, VHA has implemented physical security policies and standards as reflected in VA Handbook 0730. Throughout the years, security risk has prompted continued updates to the handbook, rendering it a living document mandating the appropriate procedural changes in an effort to protect lives and property within VA's jurisdiction. These standards consist of a wide range of security countermeasures specific to VA's culture (medical center environment) clinical and environmental management operations.

Target Completion Date: January 2019.

Recommendation 2. The Secretary of VA should develop an oversight strategy that allows VA to assess the effectiveness of risk management programs at the VHA facilities system wide.

VA Comment: Concur. VA will work with the ISC as we update our risk management process to ensure it reflects the standards established by ISC as applicable. In addition, we will evaluate the current roles and responsibilities for assessing our internal controls for risk management in order to improve our process. Target Completion Date: January 2019.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548