United States Government Accountability Office

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

VA MEDICAL CENTER SECURITY

Progress Made, but Improvements to Oversight of Risk Management and Incident Analysis Still Needed

Accessible Version

Statement of Catina B. Latham,
Acting Director, Physical Infrastructure

For Release on Delivery Expected at 2:00 p.m. ET
Tuesday, July 13, 2021

GAO Highlights

Highlights of GAO-21-105320, a testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

July 13, 2021

VA MEDICAL CENTER SECURITY

Progress Made, but Improvements to Oversight of Risk Management and Incident Analysis Still Needed

Why GAO Did This Study

The Veterans Health Administration provides critical health services to approximately 9-million enrolled veterans at its nearly 170 medical centers. Ensuring safety and security at these medical centers can be complicated because VA has to balance the treatment and care of veterans—a vulnerable population with high rates of post-traumatic stress disorder and substance abuse—while also maintaining order and enforcing the law. Officers may need to use physical force to help bring a violent or hostile situation under control.

This statement focuses on how VA manages and oversees (1) the physical security of medical centers and (2) use of force incidents by police officers. The statement is primarily based on GAO-18-201, issued in January 2018, and GAO-20-599, issued in September 2020. To update this information, GAO reviewed documentation and interviewed VA officials on actions taken to address these reports' recommendations.

What GAO Recommends

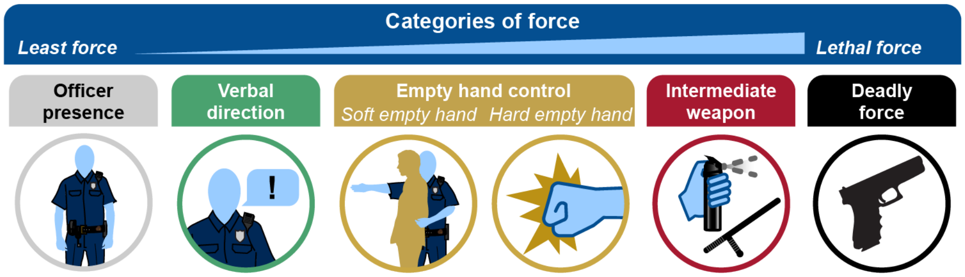
GAO made seven recommendations in its prior work, including that VA revise its risk management policies to incorporate federal standards, develop a risk management oversight strategy, improve the completeness and accuracy of use of force data, incorporate the ability to analyze incidents by facility and geographic region, and implement plans to obtain a database to collect and analyze use of force investigations. VA has made progress in addressing these recommendations. Continued attention is needed to ensure they are fully addressed.

View GAO-21-105320. For more information, contact Catina Latham at (202) 512-2834 or lathamc@gao.gov.

What GAO Found

The Department of Veterans Affairs (VA) has recently identified improvements for its physical security risk management policy and oversight process for its medical centers but has yet to implement them. In January 2018, GAO reported that VA's risk management policy did not fully reflect federal standards for facility security, such as a requirement to consider all of the undesirable events described in the standards (e.g. active shooter incidents). GAO also reported that while VA conducted some limited oversight of medical centers' risk management activities, it lacked a system-wide oversight strategy. GAO recommended that VA revise its policy to reflect federal standards and develop a system-wide oversight strategy to help to ensure that its approach to risk management will yield the appropriate security posture relative to the different risks at each of its medical centers. In response, as of June 2021, VA has begun to take actions to revise its policy to reflect the standards and fully deploy a risk assessment tool to help oversee risk management processes across medical centers. VA officials said they plan to implement the revised policy and assessment tool in fiscal year 2022.

VA has improved its data collection to support the management and oversight of police officers' use of force but could better track and analyze investigations. VA policy contains a use of force continuum scale to define and clarify the categories of force that officers can use to gain control of a situation.



Source: GAO analysis of the Department of Veterans Affairs (VA) use of force policy; Art Explosion (clip art). | GAO-21-105320

In September 2020, GAO reported that VA's records of use of force incidents were not complete or accurate. For example, GAO found that 176 out of 1,214 use of force incident reports did not include the specific type of force used. Further, VA did not track incidents by individual medical centers. GAO also reported that VA did not systematically collect or analyze use of force investigation findings from local medical centers or have a database designed for such purposes, limiting VA's ability to provide effective oversight. GAO recommended that VA improve the completeness and accuracy of its data on use of force, analyze that data by facility and geographic region, and implement plans to obtain a database to collect and analyze use of force investigations. As of June 2021, VA took steps to improve the accuracy and completeness of its use of force incident data, and officials stated VA is working to obtain a suitable database to track use of force investigation trends. GAO will continue to review VA's steps to address recommendations from both reports.

Chairman Pappas, Ranking Member Mann, and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Veterans Affairs' (VA) management and oversight of security at VA medical centers. VA's Veterans Health Administration (VHA) provides critical health services to approximately 9-million enrolled veterans at its nearly 170 medical centers. VA has faced growing demand for its health care services due, in part, to service members returning from military operations in Afghanistan and Iraq and to the growing needs of an aging veteran population. VA is expected to provide a safe environment at each of these centers, not only for the patients but also for staff and visitors.[1] Ensuring safety and security at these medical centers can be complicated because VA has to balance the treatment and care of veterans—a vulnerable population with high rates of post-traumatic stress disorder and substance abuse—while also maintaining order and enforcing the law. For example, VA police officers might respond to incidents involving disruptive patients in emergency rooms or mental health areas, which experience high levels of security incidents. In some cases, officers may need to use physical force to help bring a violent or hostile situation under control.

As of June 2020, VHA reported that approximately 5,000 VA police officers were responsible for securing and protecting VA medical centers across the country.[2] Assessing and managing risks is a critical element for ensuring adequate physical security at the medical centers. VA police officers are expected to follow a risk management process—as outlined in VA policies—to assess physical security risks and identify which

[1] We have designated federal real property management as a high-risk area since 2003, in part because of physical security challenges at federal facilities, including concerns about VA's risk management program. *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[2] VA police officers are assigned to over 130 medical centers, including medical center annexes and Community Based Outpatient Clinics. VA police provide security and law enforcement services at VHA medical centers and Veterans Benefits Administration offices co-located at those centers and may provide security for VA national cemeteries.

countermeasures each medical center needs to address those risk.[3] Countermeasures can include perimeter fencing, bollards to keep vehicles further from the building, security cameras, and access control systems. As part of the risk management process, officers are to assess a medical center's security risks by conducting biennial risk assessments.[4] VA police officers' day-to-day role at medical centers largely revolves around their law enforcement functions. The officers are authorized to carry firearms, investigate criminal activities, and arrest individuals for offenses committed on medical center property, among other activities.[5] The officers have a range of tactics they may use to control situations, including different levels of force.

My statement today focuses on how VA manages and oversees (1) the physical security of VA medical centers and (2) use of force incidents by police officers at these centers. The statement is based on reports we issued in 2018 and 2020 on VA facility security and VA police use of force, respectively, and provides an update on VA's progress towards addressing the recommendations we made in these reports.[6]

To conduct our prior work, we reviewed VA policies for VA police officers and other documents (e.g., procedures and incident reports), and also interviewed VA officials on topics related to physical security and use of force. We also reviewed documentation and interviewed officials and VA police officers from selected medical centers on these topics. We selected medical centers based on factors such as location and size.[7] While not generalizable, the selected medical centers provide illustrative examples of how VA's policies are carried out. We also compared VA's

[3] 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.

[4] VA refers to risk assessments as "vulnerability assessments."

[5] 38 U.S.C. § 902.

[6] GAO, *VA Facility Security: Policy Review and Improved Oversight Strategy Needed*, GAO-18-201 (Washington, D.C.: Jan. 11, 2018) and GAO, *VA Police: Actions Needed to Improve Data Completeness and Accuracy on Use of Force Incidents at Medical Centers*, GAO-20-599 (Washington, D.C.: Sept. 8, 2020).

[7] Specifically, for our 2018 report on VA facility security, we selected nine medical centers to include a range of patient volumes, rates of security incidents per patient, and locations, among other considerations. For our 2020 report on VA police use of force, we selected six medical centers based on factors such as the size of the facility, whether the facility was in an urban or rural area, and geographic location.

policies on physical security and use of force to federal standards for physical security and internal control, as applicable.[8] For our 2020 report on VA police use of force, we reviewed VA data on use of force incidents recorded from May 10, 2019 through May 10, 2020—the first full year of data that was available after officers were required to use VA's central recording database. As we discussed in our 2020 report and in this statement, we found limitations with this data. More detailed information on our objectives, scope, and methodology for our prior work can be found in our issued reports. For this statement, we also reviewed documents and interviewed VA officials about the actions they had taken to address recommendations made in our 2018 and 2020 reports.

We conducted the work on which this statement is based 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

Multiple entities across VA—at headquarters, regional, and local levels—have a role in carrying out, managing, or overseeing physical security activities and VA police officers (see fig. 1).

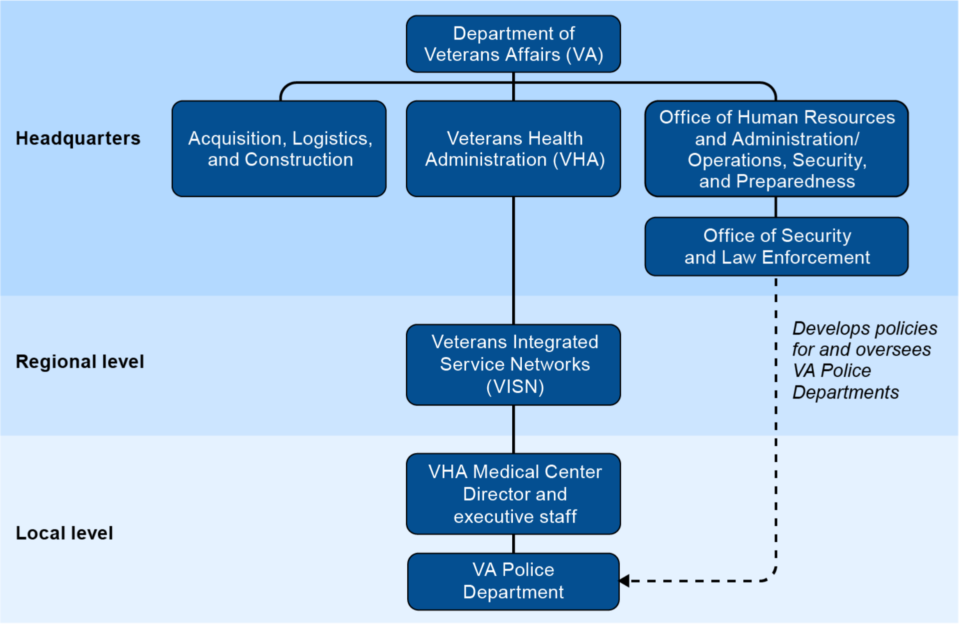
- **Headquarters:** The Office of Security and Law Enforcement (OSLE)—located within VA's Office of Human Resources and Administration/Operations, Security, and Preparedness—develops policies and standards for medical centers on physical security and VA police services. For example, the Office develops policies and standards for assessing physical security risks and law enforcement operations. The Office also conducts oversight and criminal

[8] ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D. C.: November 2016); GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: September 2014); and OMB, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123, (July 15, 2016).

investigations of medical center police units, among other responsibilities.[9]

- **Regional:** Regional Directors of 18 geographic regions called Veterans Integrated Service Networks (VISN) manage and oversee VA medical centers within their region, including the centers' physical security and police operations.
- **Local:** The primary operational responsibility for ensuring safety is at the local level, where VA police at each facility conduct risk assessments, recommend needed countermeasures, and perform law enforcement activities. The director at each medical center is responsible for implementing OSLE's policies and standards, overseeing VA police activities, and making final decisions on the appropriate countermeasures needed for their facilities.

Figure 1: Department of Veterans Affairs Entities That Are Responsible for Carrying Out, Managing, or Overseeing Physical Security Activities and Police Officers


Department of Veterans Affairs (VA)
Headquarters
Acquisition, Logistics, and Construction
Veterans Health Administration (VHA)
Office of Human Resources and Administration/ Operations, Security, and Preparedness
Office of Security and Law Enforcement
Regional level
Veterans Integrated Service Networks (VISN)
Develops policies for and oversees VA Police Departments
Local level
VHA Medical Center Director and executive staff
VA Police Department

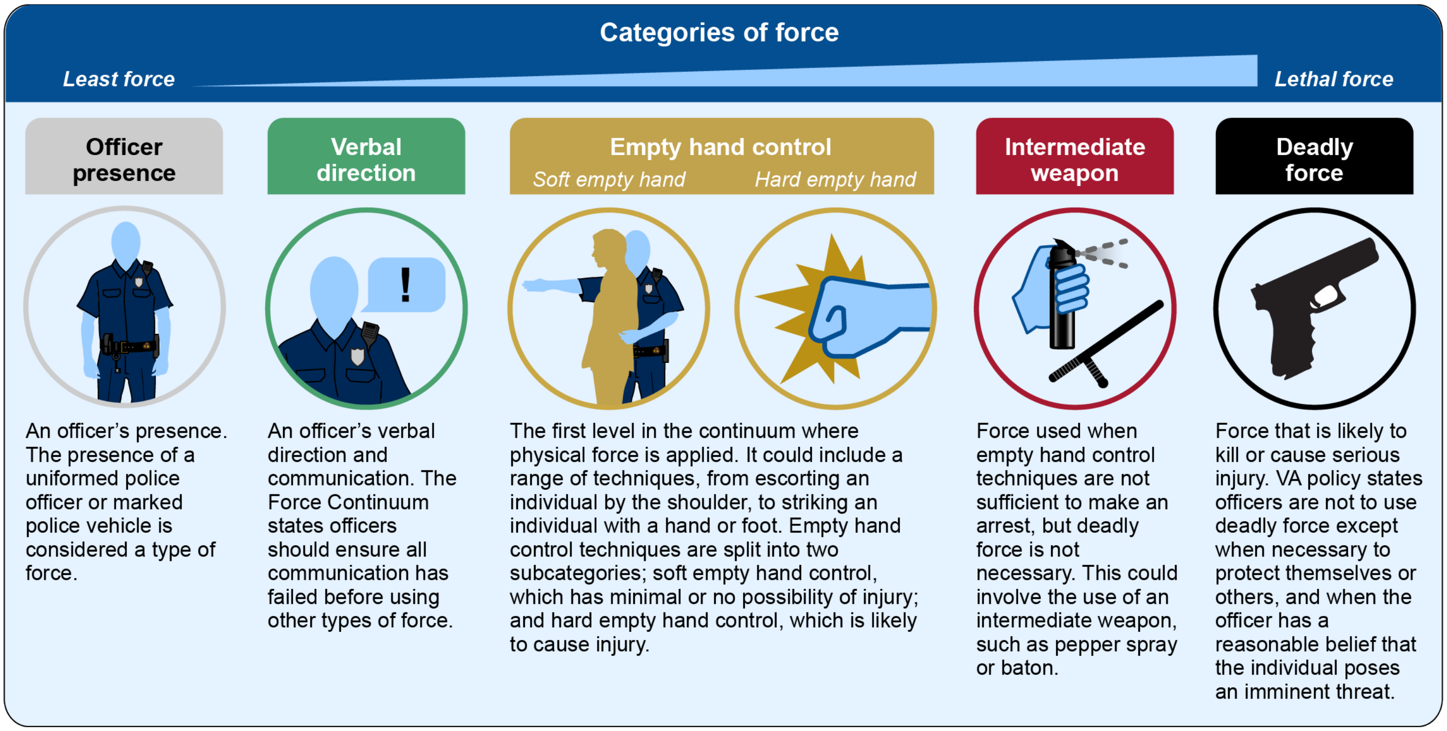
Source: GAO analysis of VA information. I GAO-21-105320

VA police are required to follow VA's *Standard Operating Procedures on Use of Force* (2007), developed by OSLE, which states that officers must

[9] In addition, in headquarters, VA's Office of Acquisition, Logistics, and Construction develops and maintains physical security design guides that specify the security requirements when constructing or leasing new medical facilities.

use only the minimal level of force that is reasonably necessary to gain control of a situation.[10] The minimal level of force is defined as the level of force least likely to cause injury that a reasonable officer would determine is necessary to bring a situation under control. OSLE has developed a Use of Force Continuum (force continuum) to define and clarify the level of force that can justifiably be used by an officer to gain control over a situation (see fig. 2).

Figure 2: The Categories of Force on the Department of Veterans Affairs Use of Force Continuum Scale



An officer's presence. The presence of a uniformed police officer or marked police vehicle is considered a type of force.

An officer's verbal direction and communication. The Force Continuum states officers should ensure all communication has failed before using other types of force.

The first level in the continuum where physical force is applied. It could include a range of techniques, from escorting an individual by the shoulder, to striking an individual with a hand or foot. Empty hand control techniques are split into two subcategories; soft empty hand control, which has minimal or no possibility of injury; and hard empty hand control, which is likely to cause injury.

Force used when empty hand control techniques are not sufficient to make an arrest, but deadly force is not necessary. This could involve the use of an intermediate weapon, such as pepper spray or baton.

Force that is likely to kill or cause serious injury. VA policy states officers are not to use deadly force except when necessary to protect themselves or others, and when the officer has a reasonable belief that the individual poses an imminent threat.

Source: GAO analysis of the Department of Veterans Affairs (VA) use of force procedures; Art Explosion (clip art). | GAO-21-105320

According to VA standard operating procedures on use of force, the force continuum is to be used as a guide for officer decisions but is not meant to overtly restrict officers' actions to protect themselves or others. Although officers should, according to the standard operating procedures,

[10] Department of Veterans Affairs, Office of Security and Law Enforcement, Standard Operating Procedures, Chapter IV, Section D (Washington, D.C.: June 2007). The use of force Standard Operating Procedures provide detailed guidance on how officers should operationalize the policies on use of force contained in VA Handbook 0720 Procedures to Arm Department of Veterans Affairs Police (2000). The Department of Justice determined that VA's use of force policy is consistent with the department's 1995 guidance on the use of deadly force by federal law enforcement.

generally escalate their use of force one level at a time to gain control of a situation, and deescalate to the level needed to maintain control, officers are not required to start at the bottom of the continuum and move through every level of force. The standard operating procedures state that using force beyond what is necessary under the particular circumstances is unjustified and considered to be a criminal act.

VA Has Identified Improvements for Its Risk Management Policy and Oversight Process, but Has Yet to Implement Them

We reported in January 2018 that VA's risk management policy did not fully reflect federal standards for facility security and that VA lacked a system-wide oversight strategy.[11] VA has since begun to update its policies to reflect federal standards and establish an oversight process.

In our 2018 report, we found that VA's risk management policy—developed by OSLE—did not fully reflect facility risk management standards established by the Department of Homeland Security's (DHS) Interagency Security Committee (ISC).[12] Those standards set forth the process federal agencies are to follow to identify appropriate countermeasures for their respective facilities and ensure their effectiveness. The process includes, for example, determining a facility's security level, assessing risk, determining necessary countermeasures, implementing the identified countermeasures, and/or expressly accepting the risk if countermeasures are not implemented. In 2018, we found that

[11] GAO-18-201.

[12] The ISC was established via Executive Order 12977 in 1995 to enhance security at federal facilities. Its mission includes developing standards and best practices. 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, 60 Fed. Reg. 54411 (Oct. 19, 1995), as amended by Executive Order 13286, 68 Fed. Reg. 10619 (Mar. 5, 2003). While only executive agencies and departments are required to follow ISC standard, ISC's standard on risk management—the *Risk Management Process for Federal Facilities*— is intended to be applicable to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities, including special-use facilities. For our 2018 report, we compared VA's polices to ISC's 2016 risk management standard because it was the most recent standard at the time of our 2018 report. See ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D. C.: November 2016).

VA's risk management policy included some elements of ISC's process but was missing other elements. For example:

- VA policy requires VA police to consider three factors (mission criticality, symbolism, and threats) when determining a facility's security level, in line with ISC standards. However, contrary to ISC standards, the policy did not require police to consider a facility's population and size. As a result, VA may not be considering all the relevant risk factors that could make a facility a more or a less desirable target for threats.
- VA's policy required VA police to conduct biennial risk assessments at each medical center, which is consistent with ISC standards. As part of these assessments, VA policy required VA police to review eight categories of threats, such as assault, physical threats of violence, and suicidal behavior. However, VA could not demonstrate how those categories relate to undesirable events (e.g., active shooter incidents) that ISC standards require agencies to consider in risk assessments. By not reviewing all the undesirable events identified by the ISC, VA may be overlooking some potential threats at its facilities.

In our 2018 report, we also found that OSLE engaged in some limited oversight of medical centers' risk management activities, but lacked a system-wide oversight strategy. As discussed, VA police at each facility are to conduct biennial risk assessments and identify countermeasures that aim to address risks. OSLE officials told us that their role in overseeing the agency's risk management process focuses on ensuring that VA police had completed their risk assessments, their annual physical security surveys that are used to inform the risk assessments, and their intruder detection tests. OSLE officials may also inspect specific areas to determine whether countermeasures that are in place meet VA's standards. However, OSLE's oversight actions did not reflect key aspects of federal standards and guidance on program effectiveness—namely *Standards for Internal Control in the Federal Government* and an Office of Management and Budget (OMB) Circular on enterprise risk management.[13] For example, federal internal control standards encourage agencies to have a process in place to ensure that their policies are being implemented as intended and to use reliable data to assess program effectiveness. We found:

[13] GAO-14-704G, OMB Circular No. A-123, updated July 15, 2016.

- OSLE confirmed that VA police completed risk assessments, but OSLE did not assess the quality of the assessments or whether the assessments aligned with VA's policy requirements.
- OSLE did not collect information system-wide that would allow it to know what security deficiencies have been identified across all medical centers and whether recommended countermeasures had been implemented.

In the absence of a comprehensive VA-wide strategy that reflects internal control and enterprise risk management standards and guidance, we found that individual sites had established their own approaches to carrying out VA's risk management policy. For example, medical centers we reviewed conducted their risk assessments differently. We also found that the lack of a system-wide oversight strategy was particularly troublesome given the authority and autonomy of medical center directors and that VA police determine the appropriate countermeasures needed for their facilities. Further, according to OSLE officials we interviewed for the 2018 report, they do not have any authority to ensure security deficiencies they identify during their inspections of medical centers are corrected. Without a system-wide oversight process, VA cannot assess the overall performance of its security program and whether medical centers are adequately protected.

Given the deficiencies we identified, we recommended in January 2018 that the Secretary of VA (1) review and revise the agency's risk management policies for VHA facilities to ensure VA incorporates ISC standards, as appropriate and (2) develop an oversight strategy that allows the agency to assess the effectiveness of risk management programs at VHA facilities system-wide.[14] In our March 2021 high risk report, we continued to identify facility security as a concern within the managing federal real property area.[15] We specifically state that the federal government may not have the capacity to conduct adequate risk assessments because agencies' security assessment methodologies, including VA's, do not fully align with the ISC's risk management process.

VA has begun to take actions to revise its policies to reflect federal standards and establish a system-wide oversight process. In June 2021, OSLE officials provided us a draft of its risk management policy that it revised in February 2021 to incorporate ISC standards. The draft revised

[14] GAO-18-201.

[15] GAO-21-119SP.

policy, for example, requires VA police to consider all undesirable events when assessing risk, in line with ISC standards. OSLE officials also told us that to help oversee the effectiveness of risk management processes across medical centers, they plan to fully deploy a tool that captures, stores, and accesses information associated with risk assessments and countermeasure recommendations at individual facilities. This tool, call the Modified Infrastructure Survey Tool 2.0 (MIST), was developed by DHS's Federal Protective Service and has been validated by ISC as following its standards. [16] OSLE officials said that, when implemented, MIST will provide them the capability to oversee the risk assessment process performed by VA police at individual medical centers and observe trends in security issues, such as vulnerabilities and repeat security incidents, at medical centers nationwide or by VISN.

As of June 2021, VA's revised risk management policy was in draft form and MIST had not been fully deployed. VA has not moved forward with implementing its revised risk management policy or MIST because it has not yet funded the purchase of the license to use MIST across police departments at medical centers or the training for all of its police officers on the revised policy and the tool. OSLE officials said that such training is required for successful implementation of the policy and tool.[17] OSLE officials said that the Office of Human Resources and Administration/Operations, Security, and Preparedness is now planning to provide the necessary funding, and that they hope to implement the revised risk management policy and MIST in the second quarter of fiscal year 2022. When OSLE implements the risk management policy and MIST, we will review their implementation to determine if they are responsive to our recommendations. Until VA implements a policy that reflects ISC standards and establishes an oversight process, it will continue to be unable to ensure that its approach to risk management will yield the appropriate security posture relative to the different risks faced at each of its medical centers. Further, without a system-wide oversight process, VA may miss opportunities to leverage resources nationally or make informed, proactive policy decisions.

[16] The Federal Protective Service is the agency primarily responsible for protecting federal employees and visitors at more than 9,000 federally owned or leased facilities, most of which are under the custody and control of GSA.

[17] According to OSLE officials, in 2020, VHA had provided some funds to train about a dozen VA police officers to test MIST at some locations.

VA Has Improved Data Collection on Use of Force Incidents but Could Better Track and Analyze Related Investigations

VA Has Taken Steps to Collect Complete and Accurate Information on Use of Force Incidents and Has Added Capabilities to Analyze Incidents

While it is critical that VA oversees medical centers’ risk assessments to ensure that centers identify appropriate countermeasures to address risks, it is also critical that VA improves oversight of its medical centers’ police units to better assess the effect of its use of force policies. We reported in September 2020 that VA’s oversight of police use of force did not involve a sufficient approach to collecting and analyzing use of force data at medical centers. However, VA has since taken steps to collect more complete and accurate data.

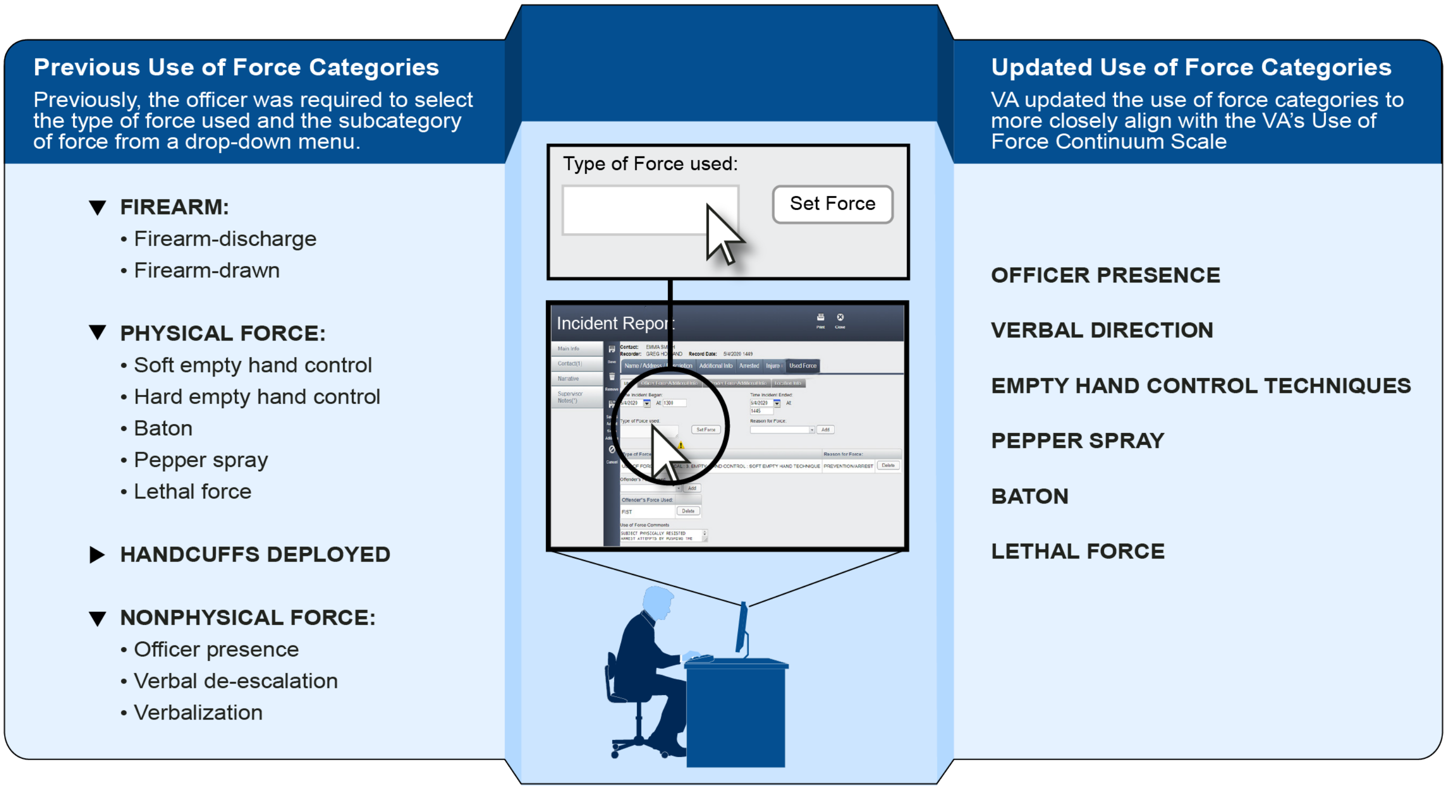
As discussed in our 2020 report, our analysis indicated that use of force data were not sufficiently complete or accurate for VA headquarters officials to develop basic descriptive statistics, including the number of use of force incidents by date and types of force used. In May 2019, VA required its police officers to complete electronic records of their daily activities, including use of force incidents in VA’s central database called Report Executive.[18] Specifically, we analyzed all 1,214 use of force incidents recorded in Report Executive from May 10, 2019, through May 10, 2020, to determine the type, frequency, and location of use of force incidents at VA medical centers. We identified three types of data issues: (1) incomplete categorization of the type of force used, (2) inaccurate data on the highest level of force used, and (3) the potential for duplicate data entries.

First, we identified incomplete categorization of use of force entries in Report Executive. Specifically, at the time of our review, an officer was required to identify from a dropdown menu which type of force was used from one of four main categories—firearm, physical force, handcuffs, or

[18] The primary electronic record is called an incident report, which contains detailed accounts of incidents occurring at a VA medical center, such as the type of incident that occurred, the time and location of the incident, whether an arrest was made, and the type of force used, if any, among other information.

nonphysical force, as illustrated on the left of figure 3. Next, the database prompted the officer to select a subcategory of force from within the applicable main category. For situations when an officer used more than one type of force during a single incident—such as using verbal commands, followed by using handcuffs—the officer was expected to enter each type of force used and then mark the highest level of force used.

Figure 3: Previous and Updated List of Use of Force Categories Available to Veterans Affairs' Police Officers When Creating an Incident Report


Previous Use of Force Categories
Previously, the officer was required to select the type of force used and the subcategory of force from a drop-down menu.
▼ FIREARM:
• Firearm-discharge
• Firearm-drawn
▼ PHYSICAL FORCE:
• Soft empty hand control
• Hard empty hand control
• Baton
• Pepper spray
• Lethal force
▶ HANDCUFFS DEPLOYED
▼ NONPHYSICAL FORCE:
• Officer presence
• Verbal de-escalation
• Verbalization
Type of Force used:
Set Force
Incident Report
Updated Use of Force Categories
VA updated the use of force categories to more closely align with the VA's Use of Force Continuum Scale
OFFICER PRESENCE
VERBAL DIRECTION
EMPTY HAND CONTROL TECHNIQUES
PEPPER SPRAY
BATON
LETHAL FORCE

Source: Department of Veterans Affairs (VA) guidance and interviews with VA officials; Art Explosion (clip art). | GAO-21-105320

Note: If the officer indicated that force was used to control a situation, the officer is required to identify from a drop down menu, which type of force was used. In September 2020, VA streamlined and reordered the use of force categories to more closely align with VA's Use of Force Continuum Scale.

Of the 1,214 records we reviewed, we found 176 records (about 14 percent) had incomplete data entries where the type of force used was not specified. VA officials told us that these inconsistencies could be the result of officers incorrectly entering the type of force used, and that errors could be minimized if the database were modified to prevent officers from submitting the use of force entries without selecting the appropriate categories and subcategories.

We also found that use of force records in Report Executive did not always identify the highest level of force used. For example, we identified 74 of the 1,214 records where officers reported using a firearm—the highest level use of force on VA's force continuum. However, in 18 of these incidents, officers identified the highest-level use of force as something other than a firearm. For instance, in 11 of the incidents involving a firearm, officers reported that deploying handcuffs was the highest level of force used. A VA official responsible for analyzing the Report Executive data told us the listing of the levels of force were not intended to be ordered from the lowest to the highest level of force, similar to the use of force continuum—rather the use of force categories were intentionally listed in alphabetical order. Given the inaccuracies we identified, conducting data analysis on the highest level of force used by officers to control incidents during this period would be misleading and incongruent with VA's force continuum.

Finally, our analysis indicated that in some limited circumstances, the same use of force incident appeared to have been recorded more than once in Report Executive. Specifically, out of the 74 use of force incidents involving firearms, we identified three instances of multiple records with the same reporting officers, date, time, and incident type. VA officials responsible for analyzing the data told us they could not determine whether the records indicated separate incidents or whether the same use of force incident was counted more than once.

In addition to the data challenges, we found that Report Executive did not allow VA officials to analyze use of force incidents by individual medical centers or geographic region. VA officials stated that Report Executive is an off-the-shelf police reporting system that was not designed to allow them to conduct comprehensive analyses on use of force incidents across medical centers, and must be configured to accommodate VA's unique reporting requirements.

According to VA's *2018-2024 Strategic Plan*, a management objective involves institutionalizing data-supported decision-making that improves the quality of the agency's outcomes.[19] In September 2020, we made five

[19] Department of Veterans Affairs, *FY 2018 – 2024 Strategic Plan*. (Washington, D.C.: refreshed May 31, 2019).

recommendations, including the recommendation that VA improve the completeness and accuracy of use of force data in Report Executive by addressing incomplete categorization of the type of force used, inaccurate data on the highest level of force used, and the potential for duplicate data entries. We also recommended that VA should implement plans to include analytical features in Report Executive that would position the agency to analyze use of force data at VA medical centers nationwide, including by officer, type of force used, and facility, among other variables.[20]

As of June 2021, VA has taken steps to address our first recommendation to improve the completeness and accuracy of the data in Report Executive, and address the potential for duplication. Specifically, VA has worked with the vendor to include a feature in Report Executive that prevents officers from submitting an incident report if the officer did not select the "type of force used" field. This validation step will help ensure officers enter the category of force used in all use of force incident reports. Further, VA worked with the vendor to streamline the 14 use of force categories and subcategories within the Report Executive database down to the six categories to more closely align with the use of force continuum from the agency's use of force *Standard Operating Procedures*, as illustrated in figure 3 above. The changes are intended to simplify the list of options officers select from when reporting the highest level of force used in an incident. In addition, VA has told us that each incident report entered into Report Executive has a unique record number assigned, and that the potential for duplicate entries is monitored at the local police station level through the report review and approval process. Lastly, VA officials stated that they addressed our second recommendation to implement the analytical features in Report Executive by working with the vendor to add the ability to analyze use of force incidents by geographic region. VA officials told us they have the ability to sort use of force incident reports by the type of force used, VISN, facility, and officer, among other variables. We are reviewing the documentation and evidence provided by VA since our report was issued to assess the extent to which these above actions address the two recommendations.

[20] GAO-20-599.

VA Has Taken Steps to Track Local Investigations but Does Not Systematically Analyze Outcomes

We reported in September 2020 that VA headquarters did not systematically collect or analyze investigations into use of force incidents. These investigations are primarily conducted at local VA medical centers when officers are found to have used an unjustified level of force. VHA and OSLE officials told us they could not be certain that they were notified of the findings of all local medical center investigations of use of force incidents. Specifically, when local investigators concluded whether an officer's use of force was justified or unjustified, Chiefs of Police may have emailed these findings to various VA offices, including the VHA or OSLE. However, VHA—the entity responsible for overseeing police activities at medical centers—did not have a policy requiring Chiefs to notify VHA of the findings of their investigations. VHA officials told us that, in practice, Chiefs typically share copies of use of force investigation findings and disciplinary outcomes with their office via email, but officials could not assure us that they received all investigation results. In contrast, Chiefs of Police are required by policy to notify OSLE—whose responsibilities are limited to developing and issuing national policies and inspecting police programs—of use of force investigations involving intermediate weapons and firearms. However, OSLE officials stated that they may not receive information on all local use of force investigations, especially those involving non-weapon-related incidents, and that the Report Executive database does not contain data on the findings or outcomes of use of force investigations.

Our September 2020 report noted that according to VHA officials, VA planned in June 2020 to draft new policies requiring Chiefs to notify VHA of all local use of force investigations and resulting disciplinary action. VHA officials also stated that VA was in the process of reorganizing the roles and responsibilities of the offices in charge of police oversight. OSLE officials stated that VA's plans for reorganizing police oversight would seek to address the collection of more complete data on use of force investigations. However, VA officials could not provide a written plan or a date by which the agency would implement such policy changes.

In addition, we reported in September 2020 that neither VHA nor OSLE systematically tracks or analyzes the outcomes of local use of force investigations across all medical centers, including disciplinary actions taken if an officer acted outside of VA's use of force policy. VA officials told us that neither VHA nor OSLE had an appropriate information system to collect and track trends in use of force investigations' outcomes, and that the Report Executive database was not configured to record use of force investigations. A senior official told us, at that time, that VHA was considering procuring a database that would, among other capacities, capture data on police use of force investigations across medical centers, including the results of those investigations, and would track any disciplinary action taken. However, VHA could not provide any documentation of such plans indicating how VA would complete such actions. OSLE officials stated that while use of force investigations are completed and documented by individual facilities and that disciplinary actions are the responsibility of the local leadership, having information on all use of force investigations would help the officials ensure that all centers are complying with the use of force procedures, and doing so in a consistent manner.

As noted above, VA's *2018-2024 Strategic Plan* involves institutionalizing data-supported decision-making by using consistent, accessible, and comprehensive data to conduct analysis to inform the improvement of outcomes for veteran services. In September 2020, our third recommendation was for VA to ensure that medical centers submit records of all locally initiated use of force investigations and any resulting disciplinary action to VA headquarters offices with responsibility for police oversight. Our fourth recommendation was that VA implement plans for obtaining a quality database to collect all locally initiated use of force investigations at medical centers. Finally, we recommended that once VA has procured its internal affairs database to collect use of force investigations, the agency analyze the investigations and any resulting disciplinary actions by facility, officer, and outcome, among other variables.

VA has taken actions to address the above three recommendations to ensure the collection of complete data on use of force investigations in a quality database in order to analyze investigation trends. In June 2021, VA officials stated that OSLE has revised and updated the VA Police use of force reporting form and mandated its use and collection across VA police force to ensure the collection of all locally initiated use of force investigations. More specifically, as of January 2021, VA police units were required to complete and submit a use of force report (form 0867h) to

OSLE personnel for review for all reportable incidents.[21] An agent assigned to the region where the incident took place reviews the use of force report and enters the information into a Law Enforcement Officer tracking report stored on an OSLE SharePoint site. The SharePoint site then sends out an automated alert to VHA and OSLE senior officials with responsibility for police oversight. The SharePoint site includes a dashboard that includes information on each use of force incident, including information on whether the officer involved was investigated, if remedial actions were taken, and whether there was an administrative or adverse action taken against the officer, among other things. The dashboard also allows VA officials to run reports to track use of force incidents by state, VISN, month, and fiscal year, and shows statistics reflecting how many adverse or administrative actions have been taken against officers, such as reprimands, written warnings, and suspensions. We are reviewing the documentation and evidence provided by VA to assess the extent to which these actions address our recommendation to ensure medical centers submit records of all locally initiated investigations to VHA and OSLE.

Regarding our two interrelated recommendations that VA procure a suitable database for and to then use it to analyze use of force investigation outcomes, VA officials reported in June 2021 that plans are still underway and that they are using the SharePoint site in the interim. To this end, VA established a working group in December 2020.[22] The working group was tasked with procuring a database to facilitate the receiving, referring, and tracking of police misconduct cases—to include excessive use of force. The proposed Internal Affairs unit would be located in VA's Office of Human Resources and Administration/Operations, Security, and Preparedness and would:

- define the professional standards for VA police units,
- expand pre-employment screenings to include employees of VA police departments, and

[21] VA form 0867h states reportable use of force incidents include the use of soft and hard empty-hand control techniques, and intermediate weapons (baton or pepper spray), as well as handgun draws, long gun deployments, and officer involved shootings. The form indicates a report is not required during the uneventful handcuffing and escorting of a voluntary compliant subject or during a routine arming/disarming and training scenarios.

[22] The group consists of representatives from the Office of Human Resources and Administration/Operations, Security, and Preparedness, Office of Security and Law Enforcement, Veterans Benefits Administration, the National Cemetery Administration, and others, according to VA officials.

- manage and conduct police misconduct investigations, among other things.

VA told us that the working group will next establish the needs, processes, ownership, and funding of the proposed Internal Affairs program based on DOJ guidelines. VA officials did not provide timelines for the completion of these steps. As for our recommendations to procure and use a suitable database, we will continue to monitor VA's progress to finalize and implement its procurement plans as well as its plans to analyze use of force investigations.

Chairman Pappas, Ranking Member Mann, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Catina B. Latham, Acting Director, Physical Infrastructure, at (202) 512-2834 or LathamC@gao.gov. You may also contact Gretta L. Goodwin, Director, Homeland Security and Justice, at (202) 512-8777 or GoodwinG@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Maria Edelstein (Assistant Director); Brett Fallavollita (Assistant Director); Melissa Bodeau; Billy Commons, Dominick Dale; Roshni Davé; Geoff Hamilton; Delwen Jones; Brendan Kretzschmar; Dainia Lawes; and Malika Rice.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO’s email updates to receive notification of newly posted products.

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, https://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, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

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

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