DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

VA Police Information Management System Needs Improvement

AUDIT

REPORT #19-05798-107

JUNE 17, 2020

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

A December 2018 Office of Inspector General (OIG) report determined VA's security and law enforcement program (police program) did not have adequate governance, due in part to confusion about roles and responsibilities between the Veterans Health Administration (VHA) and the VA Office of Security and Law Enforcement (OSLE). In response to the report, VA initiated actions to improve the national governance of its police program. A significant factor in effective police program governance, which was not within the scope of the 2018 report, is access to accurate and timely information. This includes information about arrests and investigation activities. Such information can help identify security and safety risks, determine the proper allocation of resources, and measure progress in achieving police program goals. This audit was therefore performed to determine whether VA's police information management planning and implementation strategies and systems have provided program leaders and the workforce with the information needed to manage and guide operations. Improvements in information management will help support and advance the ongoing VA efforts to strengthen police program governance.

What the Audit Found

The audit team looked at the information management strategies and systems at all 139 VA medical facilities with police units. The team found that VA did not have an effective overall strategy or plan of action to update its police information system. VA experienced significant delays in implementing an integrated, reliably performing police electronic records management system. OSLE's Law Enforcement Training Center (LETC) initiated a project in July 2015 to implement a new police records management system to replace the legacy VA Police System (VAPS) at all medical facility police units with a commercial police records management system called Report Exec. The system acquired in September 2015 was expected to be implemented at all medical facilities by the second quarter of fiscal year 2017.

As of April 2019, only 88 medical facilities (63 percent) were reportedly using the Report Exec system, while 51 facilities (37 percent) were still using VAPS, according to VA police chiefs and staff queried by the audit team. The delayed and incomplete transition created a lack of system integration. Police at VHA facilities also experienced frequent performance issues using the Report Exec system, such as lag times for accessing the system or preparing reports. Interviews and survey responses from police officers revealed that they had to switch back and forth from using the Report Exec system to VAPS to document their activities because of system performance issues. LETC mandated a transition from VAPS to the Report Exec system in May 2019 for all medical facility police units, even as police continued to experience performance issues with the Report Exec system.

The audit team found the following:

- The Report Exec system implementation was stalled for over two years.
- VHA and OSLE employees at multiple levels could not get the necessary police program information to do their jobs.
- Persistent project management and internal control weaknesses affected the VAPS replacement project.

The difficulties with the transition to the new Report Exec system, along with recurring performance issues, occurred in part because VA did not have an effective strategy or plan of action to maintain and upgrade its police information management system. Specifically, OSLE's inadequate project management processes and internal controls during acquisition and contract administration undermined the effectiveness of the police information management system.

As a result, program leaders in VHA and OSLE could not perform adequate department-wide analyses or make informed decisions on facility risks and resource allocations. Using unreliable electronic records management systems also reduced the police program's ability to provide security services because officers had to spend more time attempting to make the system work. At times, system performance issues reduced police staff availability to carry out law enforcement activities, such as patrolling medical facilities. Several police chiefs surveyed between March and April 2019 told the audit team they spent excessive amounts of time preparing reports of their activities instead of conducting patrols. Further, the lack of an effective system meant VHA could not adequately track incidents such as missing patients and use of force.

The audit team found another strategic weakness in updating VA's information management system was that LETC did not ensure information security controls were in place for the new Report Exec system. The Report Exec program manager improperly instructed VA police officers at medical facilities to use the new system to prepare incident reports without making certain the required security processes were completed. Specifically, the system had not undergone the VA-mandated risk assessment and authorization process. This process is intended to provide reasonable assurance that system-related security risks are adequately addressed, that the system is performing as intended, and that the information is protected. Incident reports, which record information pertaining to crimes or acts of serious misconduct that VA police observe or investigate, can contain sensitive personal information of employees, patients, and visitors. VA police prepared approximately 105,000 law enforcement incident reports containing sensitive personal information in the Report Exec system between December 2015 and March 2018, during which time the system was being hosted without authorization on contractor and VA servers.

This resulted in an information security vulnerability because LETC bypassed the information security provisions outlined in VA procedures and the contract; however, the OIG had not received reports of improper disclosures of these records as of December 2019. LETC also lacked support from an information security officer in the Office of Information and Technology during most of the Report Exec system implementation. Information security officers are required to ensure the security for an information system and assist with implementation and compliance with security policies. LETC managers expressed doubt as to whether their organization was appropriately positioned to manage this endeavor.

What the OIG Recommended

The OIG made six recommendations to the assistant secretary for human resources and administration/operations, security, and preparedness. The recommendations included evaluating whether LETC should serve as the manager of the records management systems for VA police, establishing a working group of subject matter experts to evaluate whether the Report Exec system meets the needs of VA police, and developing a strategy to fully implement the system or its replacement. Additional recommendations included developing and implementing a plan for resolving issues with the police records management system, and updating program procedures so they meet information management needs and requirements. The OIG further recommended that the assistant secretary initiate an agreement with the contractor to ensure information security measures are in place for police records that were stored on the contractor’s server and determine whether administrative action is appropriate for personnel involved in bypassing the information security requirements.

Finally, the OIG made one recommendation to the assistant secretary for information and technology to ensure an information security officer is consistently responsible for the Report Exec system and properly notified.

Management Comments

The assistant secretary for human resources and administration/operations, security, and preparedness and the principal deputy assistant secretary for information and technology agreed with the report recommendations. The full text of VA management comments is available in appendixes C and D. The OIG will monitor the department’s planned actions and follow up on implementation of the recommendations until all proposed actions are completed.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

COR	contracting officer's representative
DUSHOM	deputy under secretary for health for operations and management
FAR	Federal Acquisition Regulation
FY	fiscal year
GAO	Government Accountability Office
ISO	information security officer
LETC	Law Enforcement Training Center
OIG	Office of Inspector General
OIT	Office of Information and Technology
OSLE	Office of Security and Law Enforcement
OSP	Office of Operations, Security, and Preparedness
VAPS	VA Police System
VHA	Veterans Health Administration
VISN	veterans integrated service network

Introduction

A 2018 VA Office of Inspector General (OIG) report found VA's security and law enforcement program (police program) was inadequately governed, due in part to confusion about roles and responsibilities between the Veterans Health Administration (VHA) and the Office of Security and Law Enforcement (OSLE). In response, VA initiated actions to improve the national governance of its police program.[1]

Governance is the process by which VA leaders make informed decisions; provide strategic direction; and maintain accountability based on objectives, risks, and resources.[2] Information about arrests and investigation activities is vital to law enforcement agencies as they track crime trends and support critical operational decisions when managing personnel and resources. Effective program governance depends in large part on VA leaders having this information to accurately and timely identify risks and measure the achievement of program objectives.

This audit was performed to determine whether VA's police information management planning and implementation strategies and systems have provided program leaders and the workforce with the information needed to manage and guide operations. The audit team's assessment of VA's overall information management strategy focused on high-level plans and actions to maintain and update its information system, including acquisition, technical, and business process components.

VA Police Information Management

VA police collect crucial information about incidents at local facilities, such as arrests, investigations, and missing patients. This information is necessary for effective program management. VHA facility and police staff use it to analyze crime patterns, manage patrols and program resources, and determine the extent of police services.[3] Veterans integrated service network (VISN) directors also use the collected information to learn about police program activities and VA headquarters can use the information for program management. In addition, VA police refer cases that draw on that information to federal law enforcement agencies such as the offices of United States Attorneys and local law enforcement agencies for appropriate action.

The police program's information management has two parts: a paper-based process and a department-wide electronic records management system, which are both used to document information collected by VA police officers. For the latter, VA police programs used

[1] VA Office of Inspector General, *Inadequate Governance of the VA Police Program at Medical Facilities*, 17-01007-01, December 13, 2018 (updated June 10, 2019). Appendix A contains more information about the prior police audit.

[2] VA Directive 0214, *Department of Veterans Affairs Governance Structure*, August 11, 2014.

[3] VA Handbook 0730, *Security and Law Enforcement*, August 11, 2000.

two different electronic records management systems during the audit period—the VA Police System (VAPS) and the Report Exec system.

Electronic Records Management Systems

Starting in June 1994, VA police used a software package called Police and Security Version 1.0 for recording police operations and generating reports. This software package was part of the Veterans Health Information Systems and Technology Architecture. OSLE replaced the Police and Security software package with VAPS in October 2009. Based on available records and discussions with OSLE staff, the police program needed a new records management system to replace VAPS because the Office of Information and Technology (OIT) lacked knowledgeable programmers, and VAPS had high system maintenance costs. VAPS is hosted at the Austin Information Technology Center in Texas and cost approximately $101,000 for OIT to maintain from fiscal year (FY) 2015 through FY 2019, according to information from OIT staff.

In September 2015, a contracting officer awarded a contract to Omnigo Software—then known as Competitive Edge Software Incorporated—to acquire a commercial off-the-shelf records management system called Report Exec for the Law Enforcement Training Center (LETC). LETC expected the Report Exec system to be fully implemented at all medical facility police units from the fourth quarter of FY 2016 through the second quarter of FY 2017 (ending March 31, 2017). As of April 2019, the Report Exec system had not been fully implemented as expected. LETC had spent approximately $2.8 million on the Report Exec system as of the end of FY 2019, based on invoice statements and the audit team's discussions with OIT staff. These costs included contractor technical support as well as OIT support services such as application management and network support services.

Overview of Department Roles and Responsibilities

Responsibility for VA police program activities is divided between VHA and the VA Office of Operations, Security, and Preparedness (OSP). OIT provides support services for the police program's information management systems.

VHA Responsibilities

In December 2012, VA policy named the deputy under secretary for health for operations and management (DUSHOM) the senior official responsible for ensuring the police program achieves its requirements.[4]

VHA is organized into 18 regional networks called VISNs. Each VISN is led by a director who is responsible for the coordination and oversight of administrative and clinical activities at

[4] VA Directive 0730, *Security and Law Enforcement*, December 12, 2012.

medical facilities within the specified geographic network. VISN directors, who report to the DUSHOM, are also responsible for ensuring police program requirements are met within their networks. Collectively, the 18 VISNs have VA police units located in 139 VA medical facilities. Each medical facility has its own police chief.

VA police chiefs at the local medical facilities are responsible for all records and reports prepared by their units and for maintaining effective record-keeping systems. They are also responsible for implementing "legally and technically correct" law enforcement practices and physical security operations.[5] Local VA police chiefs report to their medical facility directors.

OSP Responsibilities

OSP is a VA staff office within the Office of Human Resources and Administration/Operations, Security, and Preparedness. OSLE is an element of OSP and is responsible for program oversight activities. OSLE is charged with delivering professional law enforcement and security services. Under the leadership of the executive director for security and law enforcement, OSLE has two groups—the Police Service and LETC. The Police Service group is responsible for protecting the VA Secretary and Deputy Secretary, investigating potential criminal incidents at VA facilities, and conducting inspections of medical facility police units to determine if they meet program requirements. It is also responsible for developing and issuing national police program policies, including VA Handbook 0730, *Security and Law Enforcement*, which outlines paper-based and automated processes for VA police to record and use police-related information, and procedures for performing activities such as investigations.

OSLE's LETC provides law enforcement training services for the police program and other government agencies with limited jurisdictions.[6] Training services can range from basic officer training to investigative and crime prevention instruction. LETC is a Franchise Fund Enterprise Center—a self-supporting business office that is funded by the reimbursable training services it provides to VA police officers and other agencies. OSLE, through LETC, serves as the business sponsor for the acquisition and development of VA police's department-wide electronic records management systems.[7]

[5] VA Handbook 0730; VA Directive 0730.

[6] Government agencies that use LETC as a training site include the Department of the Air Force Police, the National Institutes of Health, the National Geospatial Institute, and the Federal Bureau of Prisons.

[7] A business sponsor is the primary recipient of a product. A business sponsor's responsibilities include identifying the business's requirements, validating that they are met, and communicating progress to stakeholders.

Figure 1 illustrates the organizational structure and division of responsibilities for the police program between VHA and OSP during the audit.

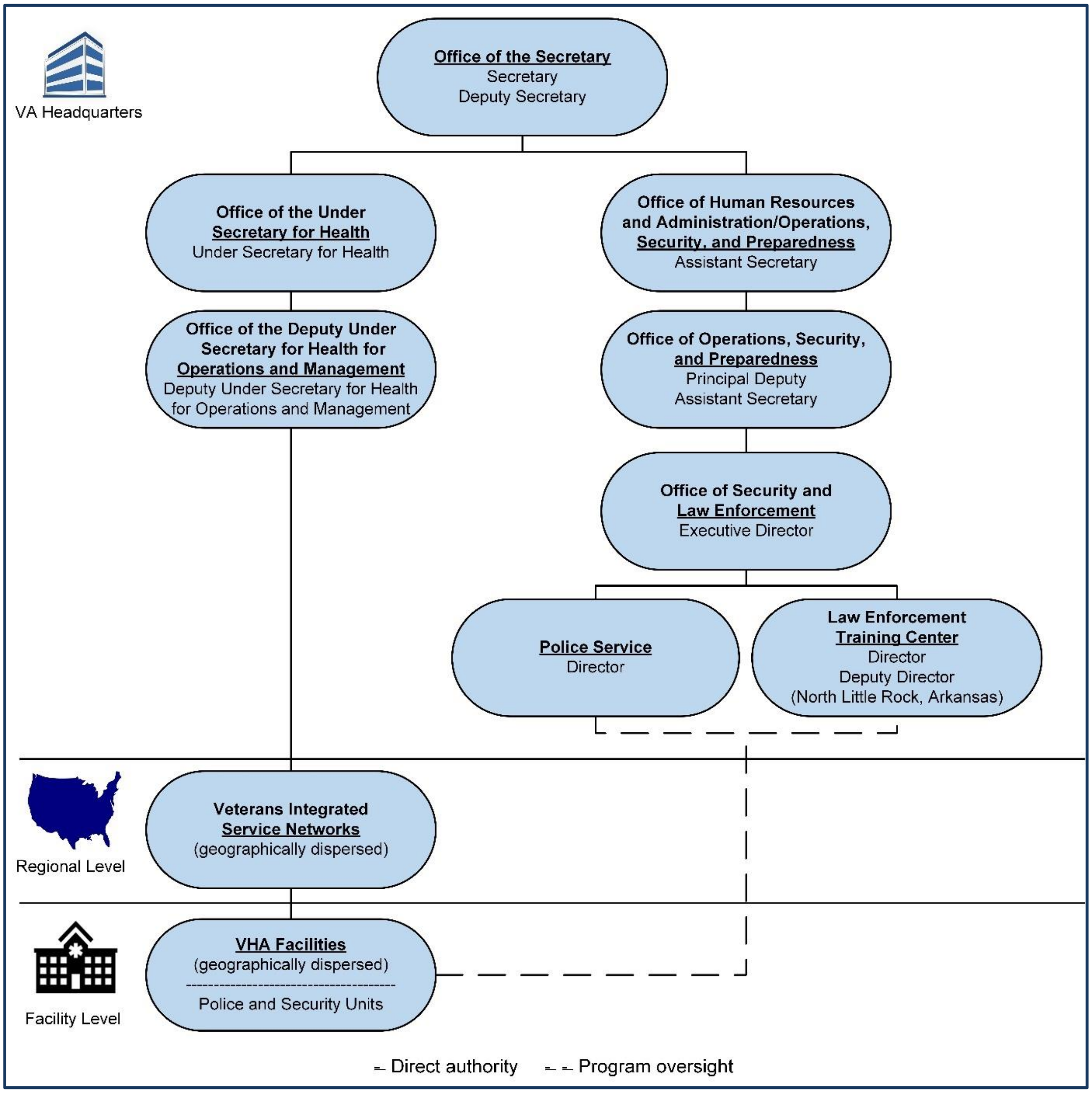
VA Headquarters
Office of the Secretary
Secretary
Deputy Secretary
Office of the Under Secretary for Health
Under Secretary for Health
Office of Human Resources and Administration/Operations, Security, and Preparedness
Assistant Secretary
Office of the Deputy Under Secretary for Health for Operations and Management
Deputy Under Secretary for Health for Operations and Management
Office of Operations, Security, and Preparedness
Principal Deputy Assistant Secretary
Office of Security and Law Enforcement
Executive Director
Police Service
Director
Law Enforcement Training Center
Director
Deputy Director
(North Little Rock, Arkansas)
Regional Level
Veterans Integrated Service Networks
(geographically dispersed)
Facility Level
VHA Facilities
(geographically dispersed)
Police and Security Units
Direct authority
Program oversight

Figure 1. *Organizational structure of VHA and OSP*

Source: OIG analysis of organizational charts and program responsibilities

OIT Responsibilities

OIT supports VA staff offices in designing, implementing, and maintaining VA's information technology systems environment.[8] OIT's IT Infrastructure Operations—which operates VA's Austin Information Technology Center—provides information technology support services to LETC through service-level agreements.[9] Services include maintenance and hosting for VAPS and the Report Exec system. According to the LETC finance division chief, LETC paid OIT approximately $5.6 million for information technology support services between FY 2009 and FY 2019.

[8] VA Directive 6518, *Enterprise Information Management (EIM)*, February 20, 2015.

[9] A service-level agreement is a contract between a service provider and a customer that details the quality and scope of the service to be provided.

Results and Recommendations

Finding 1: VA's Electronic Records Management Systems Did Not Adequately Support the Police Program

VA's police electronic records management systems did not provide program leaders and the workforce with comprehensive information at medical facilities nationwide. In September 2015, LETC acquired Report Exec, the new VA-wide records management system, to replace VAPS for VA police at all medical facilities. LETC leaders implemented the Report Exec system at medical facilities on an incremental basis and planned to have it operational by the second quarter of FY 2017. However, this resulted in a lack of system integration among the medical facilities for more than two years because individual police units were operating on different systems—VAPS and Report Exec—that did not share information. VA police at VHA facilities also reported frequent performance issues when using the Report Exec system. In May 2019, LETC leaders mandated that all medical facility police units transition to the Report Exec system and continue use of VAPS for historical information only. However, VA police continued to experience performance issues with the Report Exec system.

The audit team determined that Report Exec system integration delays and performance issues occurred because VA did not have an effective overall strategy or plan of action to update its police information management system. Strategic weaknesses were evident in project management processes and internal controls during OSLE's acquisition planning and contract administration.

As a result, program leaders in VHA and OSLE could not perform adequate department-wide analyses or make informed decisions on facility risks and resource allocations. The inconsistent performance of the Report Exec system during the transition period reduced the police program's ability to provide security services to enforce laws and protect people and property. At times, performance issues with the system prevented police staff from carrying out law enforcement activities such as patrolling medical facilities when officers had to spend time attempting to make the system work.

This finding discusses how

- The Report Exec system implementation was stalled for over two years,
- VHA and OSLE employees at multiple levels could not get the necessary police program information to do their jobs, and
- Persistent project management and internal control weaknesses affected the VAPS replacement project.

What the OIG Did

The scope of the audit focused on the effectiveness of the police program's information management strategies and systems for the 139 VA medical facilities with police units during FY 2019. The audit work included on-site fieldwork at two VA medical facilities and LETC, as well as an online survey conducted between March and April 2019. The survey asked medical facility police chiefs about their information management processes. The audit team obtained testimonial and documentary information from program officials and staff in various offices including VHA; OSP; OIT; and the Office of Acquisition, Logistics, and Construction. Appendix B provides additional details on the audit scope and methodology.

Report Exec System Implementation Was Stalled for Over Two Years

Persistent weaknesses with project management processes and internal controls stalled the full implementation of the Report Exec system until May 2019. In July 2015, LETC initiated a project to implement a new police records management system to replace VAPS at all medical facility police units. Between December 2015 and January 2016, as part of the initial implementation, LETC instructed medical facility police units to begin transitioning from VAPS to the Report Exec system. About 30 medical facility police units were involved in the initial implementation phase, which involved operating VAPS and the Report Exec system simultaneously until the information from VAPS was migrated to the Report Exec system. LETC reportedly expected the Report Exec system to be fully implemented between the fourth quarter of FY 2016 and the second quarter of FY 2017 (ending March 31, 2017).[10] The LETC deputy director confirmed to the audit team that this meant having the Report Exec system operational at all medical facilities, having the data from VAPS moved to the Report Exec system, and having VAPS decommissioned.

According to VA police chiefs and staff queried by the audit team, there were 88 VA medical facilities using the new Report Exec system (63 percent) and 51 facilities still using VAPS (37 percent) as of April 2019. This created a lack of system integration because neither records management system can share or communicate with the other to provide comprehensive police information.[11] Sharing data is necessary for VHA and OSLE leaders to generate quality information about system-wide police activities.[12] VA police also experienced frequent performance issues using the Report Exec system, such as delays accessing the system or

[10] Department of Veterans Affairs, *Franchise Fund Annual Report FY 2015*, accessed March 19, 2019, https://www.va.gov/FUND/docs/annualreports/fy15ar.pdf.

[11] Government Accountability Office (GAO), *High-Risk Series: An Update*, GAO-15-290, February 11, 2015. The GAO identified information technology challenges—the lack of system interoperability—as an area of concern in managing risks and improving health care in the VA.

[12] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014. Quality information is complete, accurate, accessible, and provided on a timely basis.

preparing reports. Interviews and survey responses from police officers revealed that they had to switch back and forth between the Report Exec system and VAPS to document their activities due to system performance issues.

As of May 5, 2019, LETC mandated that all VAPS access be deactivated and that all VA police users work in the Report Exec system. The OSP principal deputy assistant secretary told the audit team that the next planned steps include migrating VAPS legacy data and then decommissioning the system, but he did not include a time frame. He added that meetings between OIT and Omnigo about the hardware needed to back up and migrate VAPS legacy data had begun. VAPS is currently only used to obtain historical information. According to the OIT business office director, LETC spent an estimated $44,100 from FY 2017 through FY 2019 on OIT services to keep VAPS operating.

VHA and OSLE Employees at Multiple Levels Could Not Get the Necessary Police Program Information to Do Their Jobs

VA policy designated VHA's DUSHOM as the senior official responsible for ensuring police programs achieve requirements. However, in January 2019, the DUSHOM (who retired that month) told the audit team that there was no reliable system to comprehensively identify and track facility incidents involving VA police such as missing patients, traffic violations, and use of force matters. He said that information could only be obtained through ad hoc requests by VHA headquarters. In July 2019, the acting DUSHOM told the audit team that the police had moved to using one records management system, but that VHA continued to lack direct access to reliable data at the VA's central office level. She said that data were requested from OSLE and the facilities and that medical facility leaders, when appropriate, could also include police information in VHA's issue briefs.[13] According to the acting DUSHOM, the VA central office requires reliable information on police activities to identify systemic issues that need to be addressed at the enterprise level.

VA policy assigns OSLE limited responsibility for overseeing implementation and operation of the police program, such as ensuring VA police conduct investigations of alleged criminal activity.[14] OSLE, through LETC, also serves as the manager of the VA police records management systems but was unable to access needed data from either system to support its program oversight function. The executive director for security and law enforcement told the audit team that OSLE had no quick way to pull VA police information for national oversight as of October 2018 because the reporting function in Report Exec was not working at the time. He added that OSLE did not have the ability to access the archived data in the Report Exec system,

[13] VHA Directive 1004.08, *Disclosure of Adverse Events to Patients*, October 31, 2018. The directive explains that VHA uses issue briefs to report significant events.

[14] VA Directive 0730.

despite some VA police preparing information in it as early as December 2015. In September 2019, the Omnigo product manager said that there continued to be intermittent issues with the reporting function being slow or unresponsive. However, in that same month OSLE provided the audit team a report to support its national oversight role, demonstrating that the reporting function was working.

Figure 2 illustrates the design of the VA police program information management system and identifies problem areas related to the records management system components as of April 2019. Specific problem areas from top to bottom, as designated in the circles containing an "x," include: (1) the inability to access and retrieve collected information due to system problems, (2) the lack of information and communication flow between the Report Exec system and VAPS, and (3) the inability of users to obtain all necessary police information.

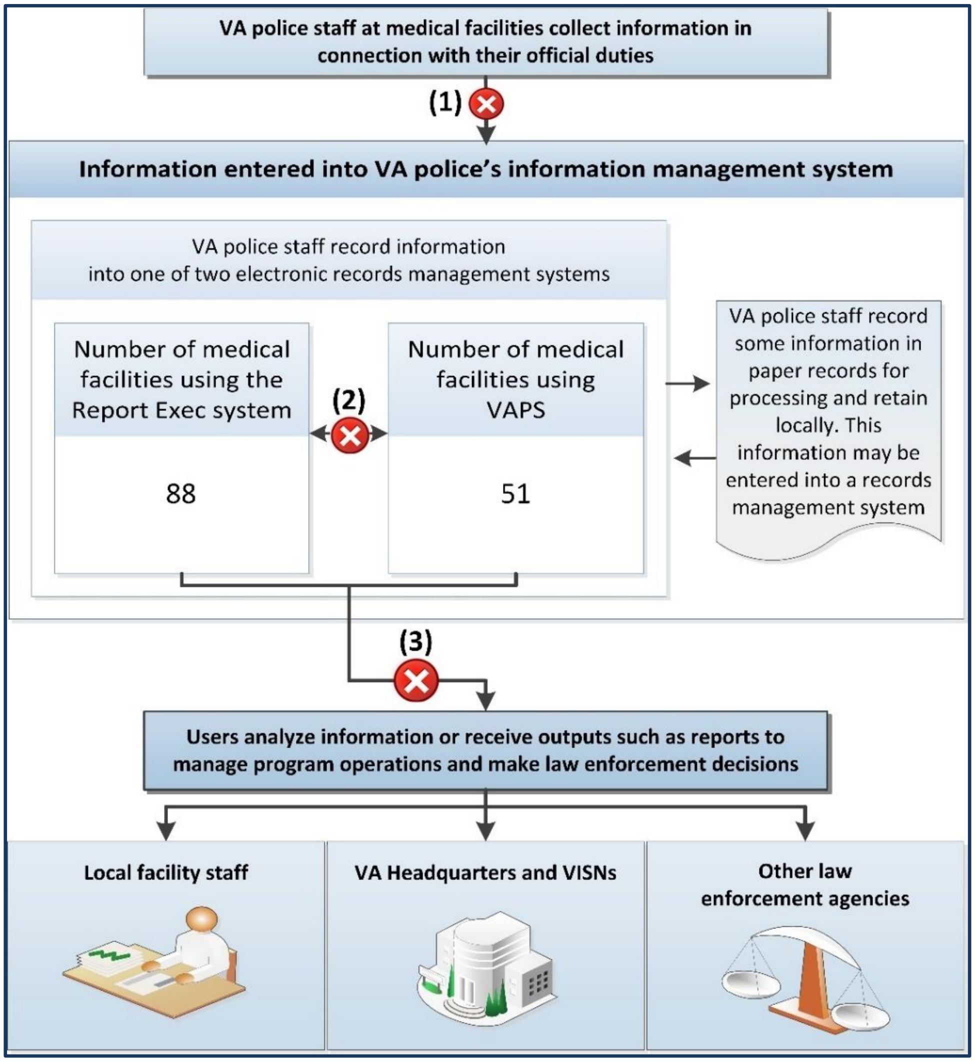
VA police staff at medical facilities collect information in connection with their official duties
(1)
Information entered into VA police's information management system
VA police staff record information into one of two electronic records management systems
Number of medical facilities using the Report Exec system
88
(2)
Number of medical facilities using VAPS
51
VA police staff record some information in paper records for processing and retain locally. This information may be entered into a records management system
(3)
Users analyze information or receive outputs such as reports to manage program operations and make law enforcement decisions
Local facility staff
VA Headquarters and VISNs
Other law enforcement agencies

Figure 2. *Overview of the police program information management system and problem areas*

Source: OIG analysis

At the facility level, the lack of an integrated records system and the Report Exec system's performance issues were sources of frustration for VA police. These issues limited the police chiefs' development of predictive criminal analyses and reduced the police program's ability to enforce laws and protect people and VA property. Police officers said they spent excessive amounts of time attempting to make the Report Exec system work to prepare reports of their activities instead of spending that time conducting patrols. Police chiefs provided comments in response to the OIG survey conducted between March and April 2019 that illustrated the frustrations about the information management systems' impact on officer time and availability:

- Some officers reported needing an undue amount of time to enter reports, with tasks that previously took 30 minutes to one hour taking "3–4 hours in Report Exec," while other officers complained that it could take "2–4 hours to write a simple report."
- "No migration from VAPS to Report Ex there fore [sic] we need to search 2 data bases for any history with VA Police."
- "The delays in officers being able to quickly enter information results in wasted time sitting in an office vs out on active patrol. It also causes unnecessary overtime as officers may stay after their tour of duty in order to try and get the report completed in a timely manner. Dispatchers have had to keep a paper journal on a regular basis that keeps data from being properly... documented and evaluated."
- "We have lost countless labor hours waiting for Report Exec to process commands. The Officers often have to keep handwritten notes on activity to enter into Report Exec once it is accessible again. Huge dis-satisfier for Police Officers. In fact, there are so many reports I have not [sic] idea what all is out there and what I am expected to track."

VA police across VHA facilities experienced recurring performance issues with the Report Exec system. For example, in June 2019, VA police staff at about 10 medical facilities expressed to the audit team that their facilities continued to experience frequent performance issues accessing the Report Exec system to prepare reports and retrieve critical information. For two weeks in August 2019, VA police nationwide were unable to log into and access the Report Exec system due to a server capacity problem.[15] In addition, some police officers experienced issues retrieving critical information about incidents that occurred at medical facilities.

[15] In response to the draft report, the principal deputy assistant secretary for information and technology clarified that the problem was caused by an application issue. (See Appendix D.)

Persistent Project Management and Internal Control Weaknesses Delayed the VAPS Replacement Project

The audit team determined that VA did not have an effective strategy or plan of action to update its police information system. The audit team identified underlying strategic weaknesses by OSLE in project management processes and internal controls during the acquisition planning and contract administration, which contributed to the system transition delays and performance issues at VHA facilities.

The OSP principal deputy assistant secretary attributed delays in replacing VAPS to the Austin Information Technology Center's inability to provide sufficient hardware resources, as well as lack of guidance and customer service. He told the audit team that LETC was just the manager and business sponsor of the system and was utilized to assist in obtaining a suitable records management system replacement.[16]

In response to questions about planning and overseeing the acquisition of the Report Exec system, the LETC director and deputy director said they questioned whether LETC should be managing the records management systems for the police program because they felt that LETC's mission focused on VA police training practices. VA policy assigns LETC responsibility for developing training policies and providing basic and specialized training for VA police officers; it does not specifically designate responsibility to LETC for police records management systems.[17] A similar concern regarding differing views about appropriate roles and responsibilities was identified in the OIG's prior audit of the police program.

Inadequate Acquisition Planning Contributed to Report Exec System Implementation Issues

Issues implementing a new commercial police records management system developed, in part, because of ineffective acquisition planning. The Federal Acquisition Regulation (FAR) states that acquisition planning is the process by which efforts are coordinated and integrated through a comprehensive plan for meeting a need in a timely manner and at a reasonable cost.[18] That planning includes developing the overall strategy for managing the acquisition. The FAR outlines the need to identify project requirements and necessary resources along with expertise and responsibility to manage the acquisition.

[16] The OSP principal deputy assistant secretary also explained that LETC, as a Franchise Fund Enterprise Center, can charge medical facility police units for using the records management systems so that LETC can recover the costs associated with the project.

[17] VA Directive 0730.

[18] FAR 2.101.

Validation of Project Requirement to Justify Acquiring a New Records Management System Was Deficient

The audit team did not validate whether discontinuing VAPS was the correct determination, but did note where there seemed to be deficiencies in the strategy to replace VAPS. On March 2, 2015, the OIT application manager at the Austin Information Technology Center reported to LETC managers that a system administrator had accidently deleted the server supporting VAPS on February 27, 2015. He also reported that it took 26 hours to rebuild and restore the data, and that most or all data from that day were lost due to the server being down and the inability to back it up.

The LETC program manager, who played a leading role in planning, acquiring, and implementing the new police records management system, told the audit team in February 2019 that LETC used the data loss incident as a catalyst to move forward with acquiring a new records management system. As part of that effort, LETC and the Strategic Acquisition Center developed a formal acquisition plan, outlining the objectives and the technical and business considerations for the acquisition. In the statement of need section, the plan stated that VAPS was "antiquated" and "failing to meet mission requirements." The plan stated that "LETC has been unable to improve the current system in a cost-effective and timely manner." In that same section, the plan also included a description of the data loss incident, stating that

> During the week of February 23–27, 2015, the LETCs [sic] current system experienced a catastrophic failure when the production server failed causing permanent loss of substantial law enforcement sensitive information. The system backups failed to restore the lost information to its original state. The loss was detrimental to the VA Police Services nationwide.

The LETC program manager signed the acquisition plan containing the above statement on July 24, 2015. He provided the audit team a copy of an email from OIT reporting the February 2015 data loss. OIT staff with direct knowledge of the event confirmed to the audit team that the February 2015 data loss occurred due to human error regarding the servers, rather than a problem with the VAPS software. The audit team concluded that including the data loss incident as support for replacing VAPS was misleading. In February 2020, the assistant secretary for human resources and administration/operations, security, and preparedness told the audit team that LETC managers did not intentionally mislead anyone about the urgency to replace VAPS. He said that the data loss incident along with continuing problems reported by staff at VA police units and the Austin Information Technology Center caused LETC to explore replacement options for VAPS.

In addition to the acquisition plan, OSLE staff told the audit team that several factors contributed to the decision to discontinue VAPS, including high maintenance and improvement costs and the lack of knowledgeable programmers in OIT. The LETC finance division chief said that OIT's continuous costs for VAPS made it difficult to manage the budget. However, the audit team determined these maintenance and improvement costs were due in part to requests by the VAPS program manager—a LETC employee who oversaw the development and maintenance of VAPS. According to the LETC finance division chief, these maintenance and improvement requests were made without notifying him first to see if the budget could accommodate them. LETC staff said that it would be more expensive to maintain VAPS than to acquire a commercial records management system. This basis might have been sufficient to justify the purchase; however, there was no documented cost analysis available to support this statement.

LETC staff also told the audit team that another factor that contributed to their decision to discontinue using VAPS was they questioned OIT's ability to deliver agreed-upon changes. As an example of these concerns, LETC referenced OIT's failure to convert VAPS to a web-based system as requested.[19] However, that change was reportedly effective as of September 2014.[20] OIT staff explained that performance issues were attributed to insufficient hardware, not the performance of VAPS.

Formal Acquisition Plan Did Not Adequately Anticipate Project Development and Needs

The audit team determined that the acquisition plan did not have adequate information concerning the project requirements, resources, and schedule for the acquisition of a new police records management system. The FAR requires that acquisition plans identify all technical, business, management, and other significant considerations that will control the acquisition.[21] LETC established a delivery schedule and performance period for the new system but did not have agreement from OIT on requirements to support the records management system and when the system could be provided. Moreover, the plan incorrectly stated that the costs for acquiring and supporting the system were "not applicable," even though the plan should have included verified costs for important components like hardware requirements to operate the system. The acquisition plan also did not address VHA staff involvement.

Project Team Was Inadequate to Support System Planning and Implementation Efforts

LETC managers did not establish an interdisciplinary team during acquisition planning with the required expertise and defined roles to ensure the project was appropriately planned and executed. The FAR requires that a team be formed during acquisition planning that consists of all

[19] A web-based system provides access to a software system using a computer and internet connection.

[20] Department of Veterans Affairs, *Franchise Fund Annual Report FY 2014,* accessed March 19, 2019, https://www.va.gov/FUND/docs/annualreports/mda14.pdf.

[21] FAR 7.105.

those who will be responsible for significant aspects of the acquisition, such as technical personnel.[22] The LETC program manager served as the project manager for the new police records management system. On July 1, 2015, the LETC project manager contacted OIT staff to inform them that LETC was acquiring a new police records management system and that OIT services would be needed to host it. However, based on the audit team's review of the acquisition plan, there was no evidence of specific hardware or network considerations for the system even though the plan and the contract stated that the system would be hosted on VA servers at OIT's Austin Information Technology Center. This would have required OIT involvement in the planning for the new system, which was lacking.

LETC did not include OIT support staff for technical support while assessing potential police records management systems and the recommended VA requirements before awarding a contract. The LETC program manager first contacted an OIT application manager with the hardware specifications on September 16, 2015, two days after the contract was awarded to acquire the Report Exec system. That application manager told the audit team that LETC did not include staff at the Austin Information Technology Center during its research for the new police system, which could have identified issues such as hardware specification requirements and the records management system's inability to connect with VA servers. The LETC program manager told the audit team that LETC officials believed they did not have to include OIT staff during their research and planning for the new system.

The project team also lacked the VAPS program manager's expert input during the acquisition planning. While the program manager oversaw the development and maintenance of VAPS, LETC staff said the VAPS program manager was excluded from being directly involved in most of the system replacement planning and implementation.[23] The audit team determined that his exclusion diminished LETC's ability to obtain reliable information about VAPS performance, such as the February 2015 data loss incident. When asked why the VAPS program manager was excluded, the LETC director explained that LETC wanted him to focus solely on VAPS.

The VAPS program manager's lack of involvement was irregular because he officially served as the contracting officer's representative (COR) for the contract to acquire the replacement records management system. As the COR, he was authorized to review contractor proposals, make recommendations to the contracting officer, and participate in negotiations. Instead, the LETC program manager reported primarily handling the planning, source evaluation, and administration of the contract, despite not officially being designated as the COR until February 2018.

[22] FAR 7.105.

[23] The VAPS program manager officially retired in April 2018.

Solicitation Process and Contract Award for the Report Exec System Omitted Data Migration

LETC conducted market research and evaluated two sources that could meet system requirements, including the capability to generate and identify reports of all incidents. LETC also held system demonstrations of different records management systems for consideration. On September 14, 2015, a contracting officer awarded a contract to Omnigo—then known as Competitive Edge Software Incorporated—to acquire the Report Exec system and its training and support services for LETC. The contract performance period was for a base year with a provision for four additional option years. The contract required Omnigo to deliver the Report Exec system within five days of the contract award. The contract also required the system to be hosted through the Austin Information Technology Center, even though LETC had not obtained a commitment from OIT to begin hosting the system at the time the system would be delivered.

According to LETC staff, the Report Exec system can perform the same functions as VAPS but also has the capability to upload photos. The Report Exec system was selected because it was the best option available at the time of the acquisition, not for any additional functions compared to VAPS. Both VAPS and the Report Exec system have the capability to track and prepare reports on various police activities such as incident reports, traffic violations, and other daily operations. Neither VAPS nor the Report Exec system was intended to track data related to VA police misconduct, so this was not considered a primary requirement.

Although the acquisition plan referenced migrating data into the Report Exec system, it was not a contract requirement. LETC managers stated they did not want to move forward with planning to transition the historical information from VAPS to the Report Exec system until it was fully implemented. The contract and subsequent modifications did not include data migration from VAPS to the Report Exec system by the contractor as a requirement.

Contract Administration Was Mismanaged

The contracting officer delegated COR authority to the VAPS program manager on September 15, 2015. According to the delegation letter, the COR is responsible for assisting with administration or performance monitoring of the contract to ensure it achieves technical requirements. This included maintaining relationships with users and contracting officers related to the project and inspecting and accepting performance and contract deliverables before authorizing invoice payments. The delegated COR is not authorized to change the scope of work, place of performance, or other conditions of the contract. The delegation letter stated that these responsibilities may not be redelegated.

The audit team determined that LETC managers improperly permitted the Report Exec program manager to assume the COR's role and authority even though the contracting officer had delegated these functions to the VAPS program manager. For example, the Report Exec program manager monitored the system's performance and acted as a liaison with the Omnigo contractor and other project stakeholders such as OIT staff and the contracting officer. However, according to LETC staff, the VAPS program manager was not involved in the acquisition planning and implementation. The Report Exec program manager said he was not initially appointed as the COR because he did not have the necessary training. He completed the required training requirements in November 2017 and was officially designated as the COR in February 2018, about 29 months after the contract was awarded.

The audit team also determined that LETC made an unauthorized agreement outside of the contract for Omnigo to temporarily operate the Report Exec system on Omnigo's servers during the initial year of the contract.[24] The audit team also determined that LETC permitted this to allow OIT time to obtain server hardware to support the system. However, the contract as signed by the contracting officer specified that the system was to be hosted at the Austin Information Technology Center. LETC entered into the agreement with Omnigo without consulting with the contracting officer. This action contributed to an information security vulnerability because LETC bypassed the required information security processes intended to ensure system-related security risks were adequately addressed, the system was performing as intended, and the information would be protected.[25]

Communication with Stakeholders Continued to Be Inefficient during Contract Administration and Project Implementation

LETC did not effectively communicate with contracting officers about performance issues it experienced during the implementation of the Report Exec system. The Report Exec program manager monitored the system's performance and communicated with the Omnigo contractor and other project stakeholders. However, the Report Exec program manager did not report any performance issues to the contracting officer or the official COR (the VAPS program manager). OSP leaders attributed performance issues to hardware problems within OIT, not the capability of the system itself. The initially assigned contracting officers told the audit team that they were not aware of any significant issues. The contracting officer at the time of this audit said that he was not informed by the Report Exec program manager about performance issues with the system until October 2018. This limited the contracting officers' ability to assess why the contractor was not meeting the contract requirements or why OIT was not providing the necessary hardware requirements. This also limited the contracting officers' ability to facilitate a resolution and determine if the contract should continue.

[24] 48 Code of Federal Regulations § 43.102. The FAR states that only contracting officers acting within the scope of their authority are empowered to execute contract modifications on behalf of the government.

[25] See Finding 2 for the OIG's determination that information security controls were not completed before the Report Exec system was operating on contractor and VA servers.

The audit team also identified three years of persistent communication challenges between LETC and OIT, including disagreements about the technical requirements for the Report Exec system, which contributed to ongoing delays in securing the necessary hardware for an integrated VA police records management system at medical facilities. Omnigo, through LETC, had provided hardware specifications to OIT support staff during the three-year period to identify the appropriate resources for an adequately performing Report Exec system. However, OIT continuously expressed divergent views to LETC about the performance of the system.

Figure 3 is a timeline from the 2015 to 2018 contract years. It provides a high-level summary of events between LETC and OIT during the Report Exec system implementation, identified by the audit team from email correspondence and contract documentation.

2015 Contract Year

- **September 14**: VA awarded the Report Exec system purchase contract to Omnigo.
- **September 16**: The Report Exec program manager contacted OIT about the hardware specifications for operating the Report Exec system. OIT had expressed that the specifications were "lite" and that there would be performance issues.
- **October 19**: Omnigo informed LETC and OIT during a meeting that new specifications and additional server hardware were necessary.
- **October 30**: Omnigo began hosting the Report Exec system for VA police, according to Omnigo.
- **December 21**: The Report Exec program manager began instructing VA police users to prepare incident reports of police activities using the Report Exec system. The Report Exec system had been rolled out to about 10 medical facilities.

2016 Contract Year

- **November 30**: Omnigo started working with LETC and OIT staff to transfer the Report Exec system and its information onto VA servers at the Austin Information Technology Center, according to Omnigo.
- **December 27–28**: The Report Exec program manager informed OIT of repeated concerns experienced by VA police users at medical facilities, including freezes and logouts. An OIT application manager expressed concern that the system might not be able to operate within VA.

2017 Contract Year

May 2–4: The OIT informed LETC staff that due to problems identifying hardware needs, it was unable to provide additional hardware before July to support the Report Exec system. The Report Exec program manager continued to express challenges experienced by VA police at medical facilities and OSLE’s inability to generate quality information about police activities system-wide.

June 5: The OIT explained to LETC staff that the Report Exec system had problems handling the medical facility processing workload, regardless of the hardware servers used.

October 11: The OIT continued to express that the Report Exec system was designed for a small business and not for the size of the VA’s police program and could not handle the requirements.

2018 Contract Year

August 9: Omnigo reported to the Report Exec program manager at LETC that the Report Exec system was still not meeting the recommended specifications to manage the number of VA police users for the system.

October 15: The LETC deputy director attempted to resolve the “communication breakdown” and challenges between LETC and OIT. He scheduled a meeting of all parties to resolve the matter. He noted that there were three years of ongoing concerns between OIT and Omnigo regarding the capability of the system and recommended requirements.[26]

Figure 3. *Timeline of events during the Report Exec system implementation*

Source: OIG analysis of email correspondence and contract documentation

Senior Manager Involvement Was Lacking in VA Police Software Oversight

Managers should perform ongoing monitoring and evaluate the results to help ensure issues are resolved promptly.[27] Even though LETC is expected to report to the executive director for security and law enforcement, project management records and the testimony of knowledgeable officials did not provide evidence that a senior executive was involved in monitoring progress and coordination between LETC and OIT, or otherwise attempting to ensure the project’s

[26] LETC continued with the implementation and mandated that all medical facility police units transition to the Report Exec system by May 2019.

[27] Office of Management and Budget Circular A-123, *Management’s Responsibility for Enterprise Risk Management and Internal Control*, Attachment, July 15, 2016; GAO, *Standards for Internal Control in the Federal Government*.

success, until October 2017. Project efforts were primarily led by the Report Exec program manager. The LETC deputy director acknowledged that while he maintained awareness of system implementation challenges and delays, he became more demanding in October 2018 to get answers about what was happening between LETC and OIT. He said that there was no specific reason for that time frame other than continued communication and accountability issues between Omnigo and OIT regarding the capability of the Report Exec system.

OSLE Established New Records Management System without Evaluating and Updating Outdated Procedures

Managers should ensure their business processes are up-to-date for continued relevance in achieving their objectives, including if there are significant changes in processes or information technology.[28] In August 2000, the VA assistant secretary for human resources and administration issued a handbook that provided mandatory procedures for recording and using police-related information. OSLE is responsible for the material contained in the handbook. The handbook, which was still in effect during the audit, had not been updated in almost 20 years to include standard guidance on the records management systems that are required to track police-related activities. For example, the handbook required recording investigation results on VA Forms 1393, but VA police were expected to record this information in VAPS or the Report Exec system. There were training and user guides developed for how to use VAPS and the Report Exec system to record police information. The executive director for security and law enforcement said that OSLE was updating the handbook to include putting all materials into one document.

Finding 1 Conclusion

The VA police program did not have a reliably performing electronic records management system in all medical facility police units that could provide leaders and police personnel with the information needed to manage and guide operations. VA did not have an effective strategy or plan of action to update its police information system. OSLE did not ensure adequate project management processes and internal controls were in place to manage such a project, and LETC managers expressed doubt as to whether their organization was appropriately positioned to undertake this endeavor.

For the police program to have a records management system that meets its future needs, VA should evaluate whether LETC is the appropriate manager for the police records management system, get stakeholder input about plans and implementation efforts, assess the suitability of the Report Exec system, develop and implement a plan to communicate and address system

[28] GAO, *Standards for Internal Control in the Federal Government*.

performance issues, and confirm police procedures keep pace with information management demands.

Recommendations 1–4

The OIG recommended that the assistant secretary for human resources and administration/operations, security, and preparedness take the following steps:[29]

1. In consultation with the under secretary for health, evaluate the appropriateness of having the Law Enforcement Training Center serve as the manager of the records management systems for VA police.
2. In consultation with the assistant secretary for information and technology, as well as the under secretary for health, establish a working group of subject matter experts and evaluate whether the Report Exec system meets the needs of VA police. The group should evaluate if the system meets police needs and whether contract requirements have been fully achieved, then develop a strategy to ensure that police units at all medical facilities have a reliably performing records management system to report and track activities.
3. In consultation with the principal executive director for the office of acquisition, logistics and construction; the assistant secretary for information and technology; and the under secretary for health, develop and implement a plan describing how, when, and to whom information about issues for the police records management system will be disseminated and resolved.
4. In consultation with the under secretary for health, update security and law enforcement program procedures to ensure they meet information management needs and requirements.

Human Resources and Administration/Operations, Security, and Preparedness Comments

The assistant secretary for human resources and administration/operations, security, and preparedness concurred with the OIG's recommendations. For Recommendation 1, the assistant secretary stated that the Office of Human Resources and Administration/Operations, Security, and Preparedness will determine the appropriate manager for the VA police records management system as part of VA's efforts to realign police operations. He anticipated implementation of this recommendation by December 2020.

[29] Recommendations directed to the under secretary for health were submitted to the executive in charge, who has the authority to perform the functions and duties of the under secretary for health.

For Recommendations 2, 3, and 4, the assistant secretary stated the Office of Human Resources and Administration/Operations, Security, and Preparedness will further evaluate and develop a strategy for the Report Exec system. He said his office will work with the Office of Acquisition, Logistics and Construction; OIT; and VHA to develop and implement a plan. He also stated that he issued a memorandum on March 10, 2020, to all staff reminding them about complying with all information security, privacy, contract security, and risk management policies. His office will work with VHA to update the applicable security and law enforcement program procedures. The assistant secretary anticipated implementation of these corrective actions by October 2020.

The full comments from the assistant secretary are included in appendix C.

OIG Response

The assistant secretary's comments and corrective action plans are responsive to the intent of the recommendations. The OIG will monitor implementation of planned actions and will close the recommendations when VA provides sufficient evidence demonstrating the proposed actions have been completed.

Finding 2: LETC Did Not Ensure Information Was Secured for the Report Exec System

Essential information security controls for the Report Exec system were not present when it initially operated. The Report Exec program manager at LETC who oversaw acquisition, planning, and implementation of the system did not make certain the mandatory risk assessment and authorization processes were completed before the system's implementation and operation. Completing the security process steps is necessary to provide reasonable assurance that risks to the system are managed, the system is functioning as intended, and data such as sensitive personal information are not vulnerable to unauthorized access.[30]

As previously mentioned, the audit team found that the Report Exec program manager instructed VA police users to prepare incident reports containing law enforcement information using the Report Exec system in December 2015, which included the sensitive personal information of employees, patients, and visitors. However, the Report Exec system was temporarily being hosted on the contractor's servers until November 2016, which caused an information security vulnerability. This finding discusses how LETC bypassed the provisions of the contract that required the system to be hosted at the Austin Information Technology Center and to be formally approved before operating. This continued from November 2016, when the system was moved to the VA servers, until March 2018, when the OIT deputy assistant secretary for enterprise program management officially authorized the system to operate—even though it had already been operating for over two years. It also highlights that LETC lacked support from an information security officer (ISO) in OIT, as required by VA procedures. Of the nearly 389,000 incident report records that were in the Report Exec system, the audit team determined that approximately 105,000 incident reports contained sensitive personal information during the two-year period without formal VA authorization.

What the OIG Did

The audit team collected documentary and testimonial information from OSP and OIT program officials and staff, as well as the product manager from Omnigo—the contractor for the Report Exec system. The audit team reviewed applicable policies and procedures and incident report data from the Report Exec system. The team obtained incident report records prepared in the Report Exec system from December 21, 2015, through March 6, 2018, that contained sensitive personal information—names in combination with dates of birth, addresses, driver's license

[30] VA Handbook 6500.3, *Assessment, Authorization, and Continuous Monitoring of VA Information Systems*, app. A, February 3, 2014. This handbook explains that sensitive personal information is any information about an individual maintained by VA, as well as information that can be used to distinguish or trace the individual's identity. Sensitive personal information is synonymous and interchangeable with personally identifiable information.

numbers, and social security numbers. Appendix B provides additional details on the audit scope and methodology.

LETC Bypassed Mandatory Information Security Procedures

The persistent project management and internal control weaknesses described in Finding 1 contributed to LETC launching the Report Exec system without formal authorization to operate. VA procedures require information systems to have formal authorization to operate before operational deployment or production status.[31] The authority for a system to operate and process information is gained through assessment and authorization processes that ensure system-related security risks are adequately addressed, the system is operating as intended, and the information will be protected. The authorizing official indicates understanding and acceptance of the risks associated with operating the system.[32] Project managers are responsible for informing VA management officials of the need to conduct a security assessment and authorization, as well as ensuring that the system receives approval to operate before deployment.

LETC managers first created an information security vulnerability in December 2015 when they bypassed VA requirements that the system be formally approved before operation. They also bypassed the information security requirement in the contract and the provision that the Report Exec system be hosted at the Austin Information Technology Center. The OIG had not received reports of improper disclosures of these records as of December 2019. The executive director for security and law enforcement could not provide documentation of who authorized this action. When the audit team asked the OSP principal deputy assistant secretary who within OSP was aware of and authorized the decision, his response did not identify any individuals:

> OS&LE is the business sponsor for Report Exec. Through the contracting and procurement process, the LETC followed the steps outlined before them via contracting rules. These rules required approval from OIT & ISO before any instructions were given to field units. Once the approvals were granted, and the contract was awarded personnel at the LETC then proceeded to assist the field as best they could.

The Report Exec program manager said that he believed the information security requirements had been completed during the acquisition process when the VA contract security checklist was completed in August 2015, a month before the contract award. The checklist is required to be completed at the initiation of all information technology acquisitions to determine the necessary security and privacy controls.[33] He also said that he was not aware of the requirement to have an

[31] VA Handbook 6500.3.

[32] VA Handbook 6500.3. An authorizing official is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk.

[33] VA Handbook 6500.6, *Contract Security*, app. A, March 12, 2010.

authorization to operate the system until later in September 2017, after a meeting with OIT. However, the contract required the completion of an assessment and authorization process—then known as certification and accreditation—since the system would be used on a VA network.

The contract security checklist was completed and first signed by the Report Exec program manager. Applicable staff including the ISO, COR, and contracting officer also signed the checklist, verifying that information security was considered for the acquisition. However, the checklist was not fully completed before they signed it. The checklist indicated that it was only an acquisition or purchase of a commodity or good but did not specify whether sensitive information was involved. The ISO at that time told the audit team that he was only involved in reviewing the checklist. He said that his information security oversight was limited because it was based on the information initially provided from LETC in the incomplete checklist.

In February 2020, the assistant secretary for human resources and administration/operations, security, and preparedness told the audit team that LETC submitted what it believed to be an accurate and complete security checklist to the subject matter experts. He reiterated that LETC was unaware it had a role in obtaining formal authorization to operate the Report Exec system until OIT staff notified LETC in September 2017.

Report Exec System Was Operating on Non-VA Servers without Authorization

The contractor, Omnigo, hosted the Report Exec system on its servers starting in October 2015 to allow VA police users at some medical facilities to use the system, according to the Omnigo product manager. The audit team determined that LETC managers permitted this so that OIT had time to obtain server hardware that would support the new system. However, one year passed before VA began hosting the system because LETC staff did not include OIT in the planning process.

Starting on December 21, 2015, the Report Exec program manager instructed some VA police users to prepare incident reports of police activities using the Report Exec system. Incident reports are used to record information about crimes or acts of serious misconduct that VA police observe or investigate. Incident reports can include the sensitive personal information of employees, patients, and visitors. For example, on December 22, 2015, a police officer at the Birmingham VA Medical Center in Alabama investigated an allegation that a patient had threatened the President. The police officer prepared an incident report in the Report Exec system that detailed how the allegation was handled, as well as personal information about the patient, including name, date of birth, address, and driver's license number. However, the Report Exec system did not have the required authorization to operate on the contractor's servers before VA police started using it, which means VA lacked assurances that the patient's information was not being put at risk.

On November 30, 2016, Omnigo started working with LETC and OIT staff to transfer the Report Exec system and its information onto VA servers, according to the Omnigo product manager. Neither LETC nor OIT could provide the audit team with reliable information to determine whether all records prepared in the Report Exec system were removed from Omnigo’s servers. The OSP principal deputy assistant secretary told the audit team that OIT was responsible for ensuring compliance with vendor servers and that OIT could provide documentation confirming this. However, OIT did not confirm this; instead, the OIT deputy portfolio director for infrastructure projects said that OIT did not have this compliance role and that LETC would need to determine whether the records in the Report Exec system were removed from Omnigo’s servers.

The Omnigo product manager told the audit team that Omnigo had access to the information entered in the Report Exec system for operational support while it hosted the system. However, he was under the impression that VA police users at the medical facilities were entering test data, not actual law enforcement information. The audit team determined that approximately 24,900 of the 105,000 incident reports containing sensitive personal information were prepared in the Report Exec system from December 21, 2015, through November 29, 2016, while it was temporarily hosted on the Omnigo servers.

Report Exec System Was Operating on VA Servers without Authorization

VA police continued using the Report Exec system once it was hosted on VA servers, still without authorization. The OIT initiated the security assessment and authorization process for the Report Exec system in October 2017, according to available records and discussions with OIT staff. By March 7, 2018, the OIT deputy assistant secretary for enterprise program management officially granted the Report Exec system an authorization to operate. When asked whether he was aware of the Report Exec system operating before his authorization, he said that he became aware of the Report Exec system in September 2017 but was unaware at the time that the system had been operating on Omnigo’s severs. The audit team determined that approximately 80,400 additional incident reports containing sensitive personal information were prepared in the Report Exec system from November 30, 2016, through March 6, 2018, when the system was operating on VA servers before it was officially authorized to operate.

LETC Lacked a Dedicated ISO through Most of the Report Exec System Implementation

VA procedures require that an ISO be assigned responsibility to ensure the security for an information system. ISOs advise and assist project managers with implementation and compliance with security policies.[34] The assigned ISO left the VA in July 2016. According to the OIT director of enterprise security operations, another OIT employee was identified as the ISO for the Report Exec system from November 2017 through October 2018. However, that OIT employee said she was not aware that she was identified as the ISO for the Report Exec system. She told the audit team that she had never been involved with the Report Exec system, only VAPS. A new ISO was confirmed as being assigned for the Report Exec system in September 2018, more than two years after the initial ISO left.

Finding 2 Conclusion

LETC improperly instructed VA police officers to operate the new system without required security protections and without authority to operate. To address information security lapses, VA needs to establish an agreement to protect VA police records stored on the contractor's servers, consider accountability for bypassing required procedures, and ensure a dedicated ISO is consistently responsible to support LETC and the Report Exec system.

Recommendations 5–7

The OIG recommended that the assistant secretary for human resources and administration/operations, security, and preparedness take the following steps:

5. In consultation with the assistant secretary for information and technology and principal executive director for the Office of Acquisition, Logistics and Construction, initiate an agreement with the contractor to ensure information security measures are in place for the VA police records that were stored on the contractor's server to prevent unauthorized use and ensure their proper disposal.
6. In consultation with the general counsel and the assistant secretary for the Office of Accountability and Whistleblower Protection, determine the appropriate administrative action to take, if any, against personnel involved in bypassing the requirement that the Report Exec system be hosted at the Austin Information Technology Center and that the VA information security process be completed before operation.

The OIG recommended that the assistant secretary for information and technology take the following step:

7. In coordination with the assistant secretary for human resources and administration/operations, security, and preparedness, ensure an information security officer is consistently responsible for the Report Exec system and properly notified.

[34] VA Handbook 6500.3.

Human Resources and Administration/Operations, Security, and Preparedness Comments

The assistant secretary for human resources and administration/operations, security, and preparedness concurred with the OIG's recommendations. For Recommendation 5, the assistant secretary stated that the Office of Human Resources and Administration/Operations, Security, and Preparedness will work with OIT to identify the appropriate information security protocols regarding data that were stored on the contractor's server. He said that his office will also work with the Office of Acquisition, Logistics and Construction to ensure information security standards and requirements that delineate responsibilities for federal personnel and the contractor are included in the contract and future contracts.

For Recommendation 6, the assistant secretary concurred but stated that it was not apparent from the OIG report and other available information that personnel engaged in willful or deliberate behavior to bypass VA information security requirements. He added that he issued a memorandum on March 10, 2020, to all staff reminding them about complying with all information security, privacy, contract security, and risk management policies. He requested closure of this recommendation based on this information.

The full comments from the assistant secretary are included in appendix C.

OIT Comments

The principal deputy assistant secretary for information and technology concurred with Recommendation 7 and stated that OIT had verified that an information system security officer was assigned to the system and notified of his responsibilities. The principal deputy assistant secretary requested closure of this recommendation based on this information.

The full comments from the principal deputy assistant secretary are included in appendix D.

OIG Response

The assistant secretary's and principal deputy assistant secretary's comments and corrective action plans are responsive to the intent of the recommendations. However, the OIG was not provided supporting documentation with the response. To close Recommendation 6, the assistant secretary for human resources and administration/operations, security, and preparedness should provide documentation demonstrating that the general counsel and the assistant secretary for the Office of Accountability and Whistleblower Protection were consulted on the matter and the decision.

Regarding Recommendation 7, the principal deputy assistant secretary for information and technology provided a screenshot showing that an information system security officer was assigned for a VA police system. To close this recommendation, the principal deputy assistant secretary should also provide documentation showing that the assigned information system security officer was notified about being responsible for the Report Exec system. In response to a technical comment (page 39) by the principal deputy assistant secretary concerning the cause of the nationwide performance issue in August 2019, the audit team updated that information in a footnote on page 10.

The OIG will monitor implementation of planned actions and will close the recommendations when sufficient evidence demonstrates the proposed actions have been completed.

Appendix A: Background

Police Program

Federal law provides the VA Secretary with the authority and responsibility to protect patients, visitors, employees, and VA property. This includes responsibility for more than six million patients receiving VA care, about 400,000 employees, and approximately 1,400 VA medical facilities and clinics.[35] VA police officers provide security and law enforcement services at VHA facilities and Veterans Benefits Administration offices colocated with VHA facilities. VA police sometimes also protect VA national cemeteries.

VA police are stationed at 139 of 141 medical facilities with police units.[36] Police officers are authorized while on or off department property to carry firearms in an official capacity and conduct investigations of offenses committed within VA's jurisdiction and consistent with other law enforcement agency agreements. They arrest individuals on department property for offenses committed within VA's jurisdiction. They also manage traffic and control parking on department property and other authorized areas.[37] In addition to the statutory requirements, VA police officers assist patients, visitors, and employees; manage physical security; and help with effective planning and use of security resources.[38]

The VA police officer workforce was reported as being among the 10 largest law enforcement organizations in the federal government.[39] VHA reported that there were approximately 5,500 VA police officers and other program staff located at geographically dispersed medical facilities as of March 12, 2019.

Prior OIG Report Concerning the Police Program

The OIG issued the report *Inadequate Governance of the VA Police Program at Medical Facilities*, 17-01007-01, on December 13, 2018, and updated it on the OIG website on June 10, 2019. The OIG concluded that VA did not have adequate and coordinated governance over its police program to ensure effective management and oversight of program requirements for its police workforce at medical facilities nationwide. The OIG found that the governance problems stemmed in part from confusion about police program roles and authority and a lack of

[35] "VA Benefits & Health Care Utilization Pocket Card," VA National Center for Veterans Analysis and Statistics, VA website, accessed October 26, 2019, https://www.va.gov/vetdata/docs/pocketcards/fy2019q4.pdf.

[36] The 141 VA medical facilities considered in the audit include medical centers, hospitals, and healthcare systems. VA medical centers and hospitals that are part of a healthcare system are supported by one police unit.

[37] Title 38, United States Code § 902.

[38] VA Directive 0730; VA Handbook 0730.

[39] Connor Brooks, "Federal Law Enforcement Officers, 2016 – Statistical Tables," Department of Justice, Bureau of Justice Statistics website, accessed May 29, 2020, https://www.bjs.gov/content/pub/pdf/fleo16st.pdf.

a centralized management or clearly designated staff within VHA to manage and oversee the police program. Among its findings, the OIG identified weaknesses including a lack of centralized operational management for its police workforce, significant police officer shortages, and lack of a quality inspection program that met prescribed timelines. In response to the report, the acting deputy secretary agreed with the recommendations and is improving the national governance of its police program, staffing levels, and the police inspection program. For example, the acting deputy secretary stated that OSP, in coordination with VHA, will take actions including conducting a comprehensive review of police programs to evaluate the need for a centralized management entity and guide any necessary changes to organizational structure, policies, and governance. The review will also help clarify program responsibilities for OSP and VHA.[40]

[40] Recommendations from the prior audit and the status of the department's corrective actions can be viewed on the OIG's report webpage.

Appendix B: Scope and Methodology

Scope

The audit team conducted its work from December 2018 through February 2020. The audit focused on the effectiveness of the police program's information management strategy and systems for the 139 VA medical facilities that had police units during FY 2019. The audit team selected two medical facilities for on-site reviews in Richmond, Virginia, and Salt Lake City, Utah. The audit included the VISNs assigned to those medical facilities visited. In addition, the audit included VHA's Office of the DUSHOM and VA's OSP in Washington, DC; OSP's LETC in North Little Rock, Arkansas; and OIT in Austin, Texas.

The audit team used multiple sources of information, including applicable regulations, VA policies and procedures, and literature on project management processes and police information management system industry practices. The team obtained testimonial and documentary information from program officials and staff in various offices across the country, including the Office of the DUSHOM, OSP, OIT, and various VA medical facilities.

Methodology

To determine whether the VA police's information management strategy and systems provided program leaders and the workforce with necessary information to manage and guide operational performance, the audit team obtained testimonial and documentary information from about 90 VHA; OSP; OIT; and Office of Acquisition, Logistics, and Construction employees about roles and responsibilities. The team interviewed management and staff about audit objective topics during site visits. The team also collected information from former VA employees and the Omnigo product manager.

The audit team conducted an online survey of 139 VA facility police chiefs on March 5, 2019, to gather information and perspectives about the specific records management system being used. This resulted in survey responses from 137 facility police chiefs nationwide as of April 5, 2019, for a response rate of about 99 percent. The team reviewed and analyzed the responses and followed up for clarification or additional information as needed.

Fraud Assessment

The audit team assessed the risk that fraud, violations of legal and regulatory requirements, and abuse could occur during this audit. The team exercised due diligence and remained alert to any fraud indicators. The team did not identify any instances of fraud during this audit.

Data Reliability

The audit team relied on computer-processed data obtained from VA's Report Exec system to identify incident report records prepared from December 21, 2015, through March 6, 2018, that contained sensitive personal information such as names in combination with dates of birth, addresses, driver's license numbers, and social security numbers. To test reliability, the team selected and compared the data with incident report documents obtained from VA medical facilities. The team believes that the data were appropriate and sufficient for the purposes in the audit based on this approach and the results of the testing.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objective. The OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

Appendix C: Management Comments, Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness

Department of Veterans Affairs Memorandum

Date: April 16, 2020

From: Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness (006)

Subj: Response to Draft Report: VA Police Information Management System Needs Improvement (Project No. 2019-05798-D2-0002)

To: Assistant Inspector General for Audits and Evaluations (52)

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG), Office of Audits and Evaluation, report "VA Police Information Management Systems Needs Improvement," Project No. 2019-05798-D2-0002. We concur with comments on the report and provide the enclosed action plan for completing the open recommendations.

The OIG removed point of contact information prior to publication.

(Original signed by)

Daniel R. Sitterly

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comments to Office of Inspector General (OIG) Draft Report, *VA Police Information Management System Needs Improvement*

(Project No. 2019-05798-D2-0002)

OIG Recommendation 1: The OIG recommends that the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Under Secretary for Health evaluate the appropriateness of having the Law Enforcement Training Center serve as the manager of the records management systems for VA police.

VA Response: Concur. On October 25, 2019, the Secretary announced a decision to realign VA police operations to increase safety and security, maintain law and order, and protect the personnel and property of the Department. Additional guidance to that decision was outlined by the Secretary in a memorandum dated February 10, 2020, referencing establishment of a national police governance body and a VA police modernization office. That memorandum also endorsed an Enterprise Integrated Project Team (IPT) to realign VA Police operations (also known as Police Modernization). Related to that effort, on February 24, 2020, HRA/OSP proposed a new organization leadership structure and a dedicated program office to support Police Modernization. The new structure includes repurposing the former OSP Principal Deputy Assistant Secretary position as the Chief Security Officer (CSO), and establishing the Office of the Chief of Police (a position that will report directly to the CSO) that will be responsible for modernizing the police force and focusing on police operations and training.

The IPT will evaluate the police records management system as one of its first taskers. Based on recommendations from the IPT, HRA/OSP, in consultation with the Veterans Health Administration (VHA), will determine the appropriate manager for the VA police records management system. Additionally, VA will augment the current Human Resources Information Technology (HRIT) governance body to include OSP IT systems. The new governance body will be known as the HRA/OSP IT Governance body, which will be chaired by the Principal Deputy Assistant Secretary, HRA/OSP, and the Principal Deputy Assistant Secretary for Management and Deputy Chief Financial Officer.

Target Completion Date: December 31, 2020.

OIG Recommendation 2: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Assistant Secretary for Information and Technology, as well as the Under Secretary for Health establish a working group of subject matter experts and evaluate whether the Report Exec system meets the needs of VA police. The group should evaluate if the system meets police needs and whether contract requirements have been fully achieved, then develop a strategy to ensure that police units at all medical facilities have a reliably performing records management system to report and track activities.

VA Response: Concur. In 2015, the LETC established a working group to discuss and guide implementation of a new police reporting system. This group consisted of representatives from the LETC, Austin Information Technology Center (AITC), Office of Information and Technology (OIT), and the VA Police Chiefs Advisory Council. HRA/OSP, in consultation with OIT and VHA, will incorporate this group’s work into the IPT to further evaluate the Report Exec system and develop a strategy for the way ahead (as referenced in the response to Recommendation #1).

Target Completion Date: October 31, 2020.

OIG Recommendation 3: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Principal executive Director for the Office of Acquisition, Logistics and Construction; the Assistant Secretary for Information and Technology; and the Under Secretary for Health develop and implement a plan describing how, when, and to whom information about issues for the police records management system will be disseminated and resolved.

VA Response: Concur. HRA/OSP will work with the Office of Acquisition, Logistics and Construction (OALC), OIT, and VHA to develop and implement a plan based on recommendations from the IPT (see responses to Recommendations #1 and #2).

Target Completion Date: October 31, 2020.

OIG Recommendation 4: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness, in consultation with the Under Secretary for Health, update security and law enforcement program procedures to ensure they meet information management needs and requirements.

VA Response: Concur. On March 10, 2020, the Assistant Secretary HRA/OSP issued a memorandum to all HRA/OSP staff providing updated guidance on the role of the Project Management Office (PMO) in HRA/OSP in exercising oversight of all contract actions within HRA/OSP. The memorandum specifically emphasizes that PMO oversight of contract actions includes compliance with all VA policies (directives and handbooks) on Information Security, Privacy, Contract Security, and Risk Management, and quality assurance / quality control of all acquisition packages. This memorandum updated prior guidance issued on January 28, 2019, which had been issued only to the HRA team. One of the purposes of this new memorandum was to include both HRA and OSP contracting actions as flowing through a single point of contact, and to also remind staff of the requirement to follow all VA policies, as noted. Using the framework in the memorandum, HRA/OSP will work with VHA to update applicable security and law enforcement program procedures.

Target Completion Date: October 31, 2020.

OIG Recommendation 5: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Assistant Secretary for Information and Technology and Principal Executive Director for the Office of Acquisition, Logistics and Construction initiate an agreement with the contractor to ensure information security measures are in place for the VA police records that were stored on the contractor’s server to prevent unauthorized use and their proper disposal.

VA Response: Concur. HRA/OSP will work with OIT to identify the appropriate information security protocols that must be adhered to regarding data that was stored on the contractor’s server. In addition, HRA/OSP will work with OALC to ensure contractual language exist in this and future contracts to ensure that Federal IT information security standards and requirements are incorporated into the contract that delineates both federal and service provider (contractor) responsibilities to ensure information security standards and followed in accordance with all federal requirements.

Target Completion Date: July 31, 2020.

OIG Recommendation 6: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the General Counsel and the Assistant Secretary for Office of Accountability and Whistleblower Protection determine the appropriate administrative action to take, if any, against personnel involved in bypassing the requirement that the Report Exec system be hosted at the Austin Information Technology Center and the VA information security process be completed before operation.

VA Response: Concur with comments. While HRA/OSP agrees that tighter controls and training reminders for staff are needed, it is not apparent that personnel engaged in willful or deliberate behavior to bypass VA information security requirements based on a review of this report and available information. As noted in the response to Recommendation #4 above, on March 10, 2020, the Assistant Secretary HRA/OSP issued a memorandum to all staff reminding them of compliance with all VA policies (directives and handbooks) on Information Security, Privacy, Contract Security, and Risk Management. Should information arise that reveals deliberate or overtly negligent bypassing of VA information security, contracting, privacy or other requirements, HRA/OSP will take appropriate administrative action against personnel involved.

Target Completion Date: Request closure based on the information above.

OIG Recommendation 7: The OIG recommended the Assistant Secretary for Information and Technology in coordination with the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness ensure an Information Security Officer is consistently responsible for the Report Exec system and properly notified.

VA Response: Concur. OIT verified in enterprise Mission Assurance Support Service, or eMASS, that an Information System Security Officer (ISSO) is assigned to VA Police Record Management System Assessing [formerly Report Exec system] and that the ISSO has been properly informed of his responsibilities.

Target Completion Date: OIT requests closure of this recommendation based on the information provided above.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

Appendix D: Management Comments, Principal Deputy Assistant Secretary for Information and Technology

Department of Veterans Affairs Memorandum

Date: April 14, 2020

From: Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer (005A)

Subj: Draft Report, *VA Police Information Management System Needs Improvement* (Project No. 2019-05798-D2-0002)

To: Assistant Inspector General for Audits and Evaluations (52)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, VA Police Information Management System Needs Improvement (Project No. 2019-05798-D2-0002). The Office of Information and Technology (OIT) concurs with OIG's findings and recommendations and submits the attached written comments. OIT requests recommendation 7 be considered closed based on the evidence of actions described in the written comments.

The OIG removed point of contact information prior to publication.

(Original signed by)

Dominic Cussatt

Attachment

Attachment

Office of Information and Technology (OIT) Comments to
Office of Inspector General (OIG) Draft Report,
VA Police Information Management System Needs Improvement
(Project No. 2019-05798-D2-0002)

OIG Recommendation 1: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Under Secretary for Health evaluate the appropriateness of having the Law Enforcement Training Center serve as the manager of the records management systems for VA police.

Comments: The Office of Information and Technology (OIT) defers to Human Resources and Administration (HRA)/ Operations, Security, and Preparedness (OSP) to respond to this recommendation.

OIG Recommendation 2: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Assistant Secretary for Information and Technology, as well as the Under Secretary for Health establish a working group of subject matter experts and evaluate whether the Report Exec system meets the needs of VA police. The group should evaluate if the system meets police needs and whether contract requirements have been fully achieved, then develop a strategy to ensure that police units at all medical facilities have a reliably performing records management system to report and track activities.

Comments: The Office of Information and Technology (OIT) defers to Human Resources and Administration (HRA)/ Operations, Security, and Preparedness (OSP) to respond to this recommendation.

OIG Recommendation 3: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Principal executive Director for the Office of Acquisition, Logistics and Construction; the Assistant Secretary for Information and Technology; and the Under Secretary for Health develop and implement a plan describing how, when, and to whom information about issues for the police records management system will be disseminated and resolved.

Comments: The Office of Information and Technology (OIT) defers to Human Resources and Administration (HRA)/ Operations, Security, and Preparedness (OSP) to respond to this recommendation.

OIG Recommendation 4: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Under Secretary for Health update security and law enforcement program procedures to ensure they meet information management needs and requirements.

Comments: The Office of Information and Technology (OIT) defers to Human Resources and Administration (HRA)/ Operations, Security, and Preparedness (OSP) to respond to this recommendation.

OIG Recommendation 5: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the Assistant Secretary for Information and Technology and Principal Executive Director for the Office of Acquisition, Logistics and construction initiate an agreement with the contractor to ensure information security measures are in place for the VA police records that were stored on the contractor's server to prevent unauthorized use and their proper disposal.

Comments: The Office of Information and Technology (OIT) defers to Human Resources and Administration (HRA)/ Operations, Security, and Preparedness (OSP) to respond to this recommendation.

<u>OIG Recommendation 6</u>: The OIG recommended the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness in consultation with the General Counsel and the Assistant Secretary for Office of Accountability and Whistleblower Protection determine the appropriate administrative action to take, if any, against personnel involved in bypassing the requirement that the Report Exec system be hosted at the Austin Information Technology Center and the VA information security process be completed before operation.

Comments: The Office of Information and Technology (OIT) defers to Human Resources and Administration (HRA)/ Operations, Security, and Preparedness (OSP) to respond to this recommendation.

<u>OIG Recommendation 7</u>: The OIG recommended the Assistant Secretary for Information and Technology, in coordination with the Assistant Secretary for Human Resources and Administration/ Operations, Security, and Preparedness, ensure an Information Security Officer is consistently responsible for the Report Exec system and properly notified.

Comments: OIT verified in enterprise Mission Assurance Support Service, or eMASS, that an Information System Security Officer (ISSO) is assigned to VA Police Record Management System Assessing [formerly Report Exec system]. The ISSO has been properly informed of his responsibilities. OIT submits the attached screenshot from eMASS as supporting evidence (Attachment A).

Target Completion Date: OIT requests closure of the recommendation based on the information provided above.

<u>OIT Technical Comment:</u>

Page 9, Final Paragraph, Third Sentence: Sentence reads:

"VA police experienced a nationwide performance issue for two weeks in August 2019 when they were unable to log into and access the Report Exec system due to a server capacity problem."

<u>OIT Comment</u>: The above is an inaccurate statement, as the problem was not due to a server capacity issue but an application issue that was resolved with an application code fix on both the application side and the database side of the environment. As evidence supporting the above technical comment, OIT submits the Omnigo Software Report Exec Stability Issues Root Cause Analysis (Attachment B).

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Audit Team	Steven Wise, Director Dustin Clark Emily Marcus Jason Ramserran Michelle Swagler Brandon Thompson Leslie Yuri

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Office of Human Resources and Administration/Operations, Security, and Preparedness
Office of Information and Technology

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.va.gov/oig.