US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Noncompliance with Contractor Employee Vetting Requirements Exposes VA to Risk

Audit | **21-03255-02** | **February 8, 2024**

BE A
VOICE FOR VETERANS
REPORT WRONGDOING
vaoig.gov/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

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.

Executive Summary

The VA Office of Inspector General (OIG) performed this audit to assess Department of Veterans Affairs compliance with executive orders, federal regulations, and VA requirements for vetting contractor employees. Every contractor employee must be vetted before beginning work at VA. The vetting requirement was established to ensure all contractor employees performing work for or on behalf of the government are and continue to be loyal to the United States, reliable, trustworthy, and of good conduct and character—in other words, fit to serve. If the vetting process discloses criminal activity, character issues, or false statements, the applicant might be rendered ineligible from working on a government contract.

Contractor employee vetting requirements are prescribed by executive orders and federal regulations.[1] They include a risk and national security sensitivity designation, fingerprint check, background investigation, evaluation, and adjudication.[2] Federal regulation does not require a sensitivity designation or background investigation if a person works for 180 days or less in a calendar year.[3] However, VA policies require all contractor employees, including those working 180 days or less, to complete a fingerprint criminal history check.

To help agencies assign risk and sensitivity levels in a systematic and uniform way, the Office of Personnel Management provided agencies with a position designation automated tool. The tool generates a position designation record, which identifies the risk and sensitivity levels for each position, which in turn determine the position's investigative requirements.

What the Audit Found

The audit team selected 50 service contracts throughout VA that were issued between January 1 and December 31, 2020, and found that VA officials had a high rate of noncompliance with executive orders, federal regulations, or VA policies for vetting contractor employees. The team found that 47 of 50 contract files (94 percent) did not include position designation records that established the position investigative requirements for the contract. In addition, 34 of 50 contracts (68 percent) did not include contract language to communicate contractor vetting requirements to the contractor. Ultimately, 215 of the 286 contractor employees reviewed (about 75 percent) did not have evidence of completed fingerprint checks, and 225 of the 286 contractor employees (about 79 percent) did not have evidence that a background investigation was completed by an investigative service provider.

[1] Exec. Order No. 13764, 5 C.F.R. § 731 (January 1, 2017).

[2] Exec. Order No. 13764; "Background Evaluation/Investigation" (web page), Office of Personnel Management, accessed July 1, 2022, https://www.opm.gov/policy-data-oversight/assessment-and-selection/other-assessment-methods/background-evaluationinvestigation/.

[3] 5 C.F.R. § 731.104.

Several VA offices have responsibility for the department's suitability program, starting with the Office of Human Resources and Administration/Operations, Security, and Preparedness (HRA/OSP). HRA/OSP is responsible for establishing and maintaining personnel suitability programs throughout the department, including developing, coordinating, and overseeing the implementation of policy and guidance. In addition, the Office of Information and Technology is responsible for implementing a department-wide information security program to protect VA information resources. Furthermore, the Office of Acquisition, Logistics, and Construction (OALC) is responsible for ensuring that VA complies with all acquisition laws and policies. To help acquisition professionals comply with laws and regulations, OALC issues policies and direction in the VA Acquisition Regulation and VA Acquisition Manual.

HRA/OSP and the Office of Information and Technology issued five directives and handbooks that discuss requirements for vetting contractor employees. The five directives and handbooks are outdated and include conflicting or inaccurate information regarding the roles and responsibilities for vetting contractor employees. While the HRA/OSP and the Office of Information and Technology are updating their respective directives and handbooks, HRA/OSP senior officials initially disregarded formal comments on the updated policies on the roles and responsibilities from OALC, the subject matter expert for acquisition matters within VA.[4] Compounding the issue, OALC issued guidance to the VA acquisition professionals directing them to the wrong policies.

Noncompliance with contractor employee vetting requirements puts VA at risk. Specifically, unvetted contractor employees increase the risks to the health and well-being of veterans and VA employees, as well as the efficiency and integrity of VA services, government property, and information. For example, the team's review of a contract for unarmed security guards at the St. Cloud VA Medical Center in Minnesota determined that officials did not vet any of the 73 contractor employees, 38 of whom (about 52 percent) had criminal records. The criminal records included arrests and convictions ranging from petty misdemeanors to felonies such as disorderly conduct, domestic abuse, physical and sexual assault, financial card fraud, and terroristic threats. During the performance of the contract, VA police, St. Cloud officials, and the VA OIG were notified about improper behavior by the unvetted contractor employees, including stalking female VA and contractor employees, sexually harassing and assaulting other employees, getting into altercations at the medical center that required police intervention, and bragging to coworkers about being a gang member. Unless VA improves compliance with federal regulations and executive orders and updates and clarifies its internal policies and procedures for vetting contractor employees, VA may hire other contractor employees who could put employees, veterans, information, and information systems at increased risk.

[4] In July 2023, an HRA/OSP senior official stated that HRA/OSP staff misinterpreted OALC's comments. Based on communication from the OIG, HRA/OSP reopened discussions with OALC about the comments and updated the draft policies accordingly.

What the OIG Recommended

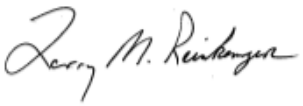
The OIG made six recommendations. Because of long-standing disagreements between HRA/OSP and OALC concerning roles and responsibilities for personnel security, the OIG recommended the VA Deputy Secretary mediate their efforts to collaborate on developing and publishing updates to the policies and procedures for vetting contractors. The OIG further recommended that the assistant secretary for HRA/OSP conduct compliance inspections of the vetting and credentialing procedures used at the St. Cloud VA Medical Center in Minnesota. The OIG also recommended the executive director of the Office of Acquisition and Logistics update and publish the VA Acquisition Regulation and VA Acquisition Manual to direct acquisition professionals to the correct policies for vetting contractor employees. The assistant secretary for information and technology should also update and publish VA Handbook 6500.6, in collaboration with officials from OALC and HRA/OSP, to ensure that the handbook does not include personnel security procedures that are discussed in other policies.

VA Management Comments and OIG Response

The Deputy Secretary concurred with the OIG's findings, concurred in principle with recommendation 1, and concurred with recommendations 2 through 6.

For recommendation 1, the Deputy Secretary stated that HRA/OSP established and communicated standardized contractor vetting processes. The Deputy Secretary also stated that contract clauses are in place and that various policies and clauses are continuously reviewed and updated when necessary. Although the Deputy Secretary agreed with the recommendation, the comments were not fully responsive. VA's five directives and handbooks that discuss vetting contractor employees remain outdated, conflicting, and inaccurate. The OIG also highlighted ineffective collaboration between HRA/OSP and OALC. For these reasons, the OIG believes it is necessary that the Deputy Secretary take an active and ongoing role in ensuring HRA/OSP and OALC officials develop and publish the necessary personnel security policy and procedure updates for vetting contractor employees as stated in the recommendation. Accordingly, the recommendation will stay open until VA demonstrates sufficient progress on the implementation and fulfillment of the recommendation's intent.

The Deputy Secretary provided responsive action plans for recommendations 2 through 6. For recommendations 1, 2, 3, and 5, the OIG will monitor VA's progress on its proposed actions and will close the recommendations when documentation has been provided to demonstrate sufficient progress on implementation and fulfillment of the recommendations' intent. For recommendations 4 and 6, the OIG considers these actions responsive and closed these recommendations based on the actions and documentation provided. Appendix C includes the full text of the Deputy Secretary's comments.



LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

HRA/OSP	Human Resources and Administration/Operations, Security, and Preparedness
OALC	Office of Acquisition, Logistics, and Construction
OIG	Office of Inspector General
OIT	Office of Information and Technology
PDT	position designation automated tool
VAAM	VA Acquisition Manual
VAAR	VA Acquisition Regulation
VA-CABS	VA Centralized Adjudication Background Investigation System
VHA	Veterans Health Administration

Introduction

As of March 2023, VA had 41,116 credentialed contractor employees performing services including veteran health care, childcare, security, medical disability examinations, and janitorial work. Contractor employees must be vetted through a background check and other methods before gaining access to VA facilities, information, information systems, staff, or other assets of the federal government. Federal regulations and executive orders established contractor employee vetting requirements to ensure contractors are loyal to the United States, reliable, trustworthy, and of good character and conduct—in other words, fit to serve.

Contractor employees are subject to the same vetting standards, policies, and procedures as civil service employees. Specifically, contractor employee vetting includes the designation of risk and sensitivity for all positions, a fingerprint criminal history check, a background investigation, evaluation, and adjudication.[5] If vetting uncovers crimes, character issues, or false statements, among other issues, a person may be disqualified from working for or on behalf of the government.[6]

If contractor employees are not vetted prior to working for VA, they may pose a risk to veterans' and VA employees' safety, as well as the efficiency and integrity of VA services, government property, or VA information. The VA Office of Inspector General (OIG) performed this audit to assess VA's compliance with executive orders, federal regulations, and VA requirements for vetting contractor employees to serve on VA contracts.

Federal Requirements for Vetting Contractor Employees

Determining suitability or fitness to serve in federal government positions has been required for over 75 years. In 1947, an executive order was issued to ensure those employed in the federal service had "complete and unswerving loyalty to the United States."[7] That principle has been expanded to ensure those working for or on behalf of the federal government are reliable, trustworthy, and of good conduct and character.[8] To uphold the principles of suitability or fitness to serve the federal government, federal regulations and a series of executive orders created requirements that apply to those performing work for or on behalf of any agency, whether through direct employment or under a contract between a nonfederal entity and any federal agency, or under a subcontract between two nonfederal entities.

[5] Exec. Order No. 13764, 82 Fed. Reg. 13 (Jan. 17, 2017).

[6] 5 C.F.R. § 731.202; 5 C.F.R. § 731.203.

[7] "Executive Order 9835" (web page), Harry S. Truman Library, accessed February 1, 2022, https://www.trumanlibrary.gov/library/executive-orders/9835/executive-order-9835.

[8] Exec. Order No. 13764.

Federal regulation requires that individuals appointed to covered positions be vetted for suitability to serve in the federal government.[9] A covered position is one in the competitive service, excepted service (people hired through other than traditional, competitive hiring procedures) where the incumbent can be noncompetitively converted to the competitive service, or a career appointment to the Senior Executive Service. All other excepted service positions, contractor positions, and nonappropriated fund positions are subject to the same investigative requirements by executive order.[10] The vetting process works to ensure the individual is, and remains over time, suitable or fit for federal employment, and where pertinent, is eligible to occupy a sensitive position, access classified information, serve as a contractor, and be issued a federal credential.

Pursuant to the federal regulations and executive orders, contractor employees are subject to two main requirements: (1) risk and national security sensitivity designations of the contracted positions and (2) investigation, evaluation, and adjudication of the contractor employees' background or fitness to serve. Figure 1 shows the key steps for vetting contractor employees.

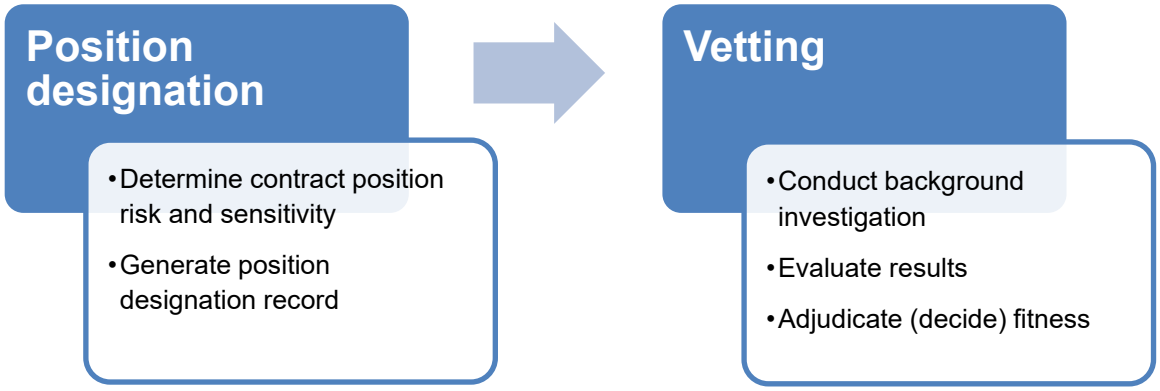


Figure 1. *Requirements for vetting contractor employees.*
Source: VA OIG analysis of federal regulations.

Risk and Sensitivity Designations of Position

Federal regulations, applied to contractors by executive order, require agencies to designate every contractor position with a risk level.[11] The same authorities mandate that all contractor positions subject to investigation also receive a national security sensitivity designation.[12]

To ensure all positions are designated in a systematic, dependable, and uniform way, the Office of Personnel Management and the Defense Counterintelligence and Security Agency provide

[9] 5 C.F.R. § 731.101.
[10] Exec. Order No. 13764.
[11] 5 C.F.R. § 731.104; 5 C.F.R. § 731.106; Exec. Order No. 13764.
[12] 5 C.F.R. § 731.104; 5 C.F.R. § 731.106. Positions that do not exceed 180 days in a calendar year do not require a background investigation and are therefore exempt from the requirement for a position sensitivity designation.

agencies with the position designation automated tool (PDT). The PDT assigns each position a risk level and national security sensitivity designation, which determine the level of investigation required for the position.[13] The risk level can be high, moderate, or low in accordance with the position's potential for adverse impact to the efficiency or integrity of the service. For example, public safety and law enforcement positions would be classified as moderate or high risk, while positions like landscaping would be classified as low risk. National security sensitivity designations are complementary to the risk level and may influence the position's investigative requirements. Sensitivity designation categories include noncritical sensitive, critical sensitive, and special sensitive. These designations are applied to positions based on the degree of risk for potential damage to national security.

Contractor Employee Investigation and Adjudication

Contractor employees are vetted through a fingerprint criminal history check, a background investigation, evaluation, adjudication, and ongoing assessments to ensure each individual continues to meet the standards for fitness for the position.[14]

Fingerprint Check

To conduct a fingerprint criminal history check, referred to as a special agreement check, agencies obtain the candidate's fingerprints and submit them for a Federal Bureau of Investigation criminal history check. This check provides a degree of assurance that the individual is not subject to an ongoing inquiry or does not have a prior criminal conviction that could affect fitness for the position. The screening is generally completed before employment but may be adjudicated up to five days after the contractor employee's start date.

Background Investigation

Background investigations are conducted by the government's investigative service provider, the Defense Counterintelligence and Security Agency, to gather information about a person's behavioral reliability, integrity, and mental health.[15] The investigations determine whether any information obtained would indicate a problem with an applicant's fitness to hold the position, including violations of statutes, regulations, or laws. The information gathered includes employment, criminal, and personal history collected from the applicant and sometimes other sources, such as former employers, coworkers, friends, and neighbors. At a minimum, background investigations include (1) a name check conducted by the Federal Bureau of

[13] 5 C.F.R. § 731.106.

[14] Exec. Order No. 13764.

[15] "Personnel Security" (web page), Defense Counterintelligence and Security Agency, accessed July 1, 2023, https://www.dcsa.mil/About-Us/Directorates/Personnel-Security/.

Investigation and using other federal databases and (2) written inquiries to employers, candidate-supplied references, and places of education and residence.[16]

Federal regulation exempts certain positions from background investigation requirements, including positions that are intermittent, seasonal, per diem, or temporary, not to exceed an aggregate of 180 calendar days per year in either a single continuous appointment or a series of appointments.[17] However, federal regulation states that the agency must conduct other checks that it deems appropriate to ensure a person's suitability or fitness. Accordingly, VA requires all contractor employees, even those exempt from background investigations, to complete a fingerprint check.[18]

Evaluation and Adjudication

Information gathered during the background investigation, as well as any other available information that is relevant and reliable, is used to evaluate and ultimately adjudicate (decide) a contractor employee's fitness to serve. Adjudication results in a determination, which is the decision made by an agency as to whether the contractor employee has the required level of character and conduct necessary to work for or on behalf of a federal agency. Specific factors considered are

- misconduct or negligence in employment;
- criminal or dishonest conduct;
- a materially false statement or deception in examination or appointment;
- alcohol abuse, without evidence of rehabilitation, of a nature and duration that suggests the applicant would not be able to perform the duties of the position or would be a direct threat to the property or safety of others;
- illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;
- knowing and willful engagement in acts or activities designed to overthrow the US government by force; and
- any statutory or regulatory bar which prevents the lawful employment of the person involved in the position.[19]

[16] VA Directive 0710, *Personnel Security and Suitability Program,* June 4, 2010; VA Handbook 0710, *Personnel Security and Suitability Program*, May 2, 2016.

[17] 5 C.F.R. § 731.104.

[18] VA Handbook 0710.

[19] 5 C.F.R. § 731.202; Exec. Order No. 13764.

To process background investigations and track suitability-related data, VA uses its Centralized Adjudication Background Investigation System (VA-CABS), a commercial off-the-shelf product. VA-CABS was launched in April 2019 and captures data about fingerprint checks, background investigations, and reinvestigations. VA plans to replace VA CABS with a customizable system, named VA-CABS 2.0.[20] As of May 2023, VA did not have a definitive go-live date for VA-CABS 2.0.

VA Policies and Responsible Offices

To implement the requirements from the executive orders and federal regulations, VA issued its own policies for vetting contractor employees. In addition, several organizations are responsible for establishing policies and vetting contractor employees.

Policies

VA Directive and Handbook 0710, *Personnel Security and Suitability Program,* define criteria and procedures for making suitability and contractor vetting determinations in accordance with federal regulations.[21] Specifically, the directive and handbook define program roles and responsibilities and procedural requirements for background investigations of contractors. VA also issued a directive and handbook laying out identity, credential, and access management policies.[22]

Furthermore, VA issued acquisition policies to the department in the VA Acquisition Regulation (VAAR), which implements and supplements the Federal Acquisition Regulation. These regulations apply to all VA acquisitions and establish uniform policies and procedures for VA's acquisition of supplies and services. In addition, the VA Acquisition Manual (VAAM) establishes guidance for how the VA acquisition workforce will follow federal and VA acquisition regulations, including those applicable to the vetting of contractors.

Responsible Offices

The director of the Office of Personnel Management is the suitability and credentialing executive agent for the federal government. As the executive agent, the director is responsible for defining minimum suitability and fitness standards, position designation

[20] VA OIG, *VA's Governance of Its Personnel Suitability Program for Medical Facilities Continues to Need Improvement*, Report No. 21-03718-189, September 21, 2023. The report indicated VA did not provide effective governance of the personnel suitability program to ensure that required background investigations were completed for staff at medical facilities nationwide. In addition, VA's systems and data did not adequately support the suitability program.

[21] VA Directive 0710; VA Handbook 0710.

[22] VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, October 26, 2015; VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, March 24, 2014.

requirements, investigative standards, policies, and procedures, and for making suitability determinations. In addition, the director is required to continually review agency programs for suitability and fitness vetting to determine whether they are implemented in accordance with executive orders and federal regulations.

The Defense Counterintelligence and Security Agency is the federal government's largest security agency and the primary investigative service provider for the federal government. In this role, it conducts 95 percent of all background investigations for more than 100 federal agencies.

Several VA leaders have responsibility for the department's suitability program, starting with the assistant secretary for Human Resources and Administration/Operations, Security, and Preparedness (HRA/OSP).[23] According to VA guidance, this position has the authority to establish and maintain personnel suitability programs throughout the department consistent with applicable laws, rules, regulations, and executive orders.[24] The Office of Identity, Credential, and Access Management, under HRA/OSP, is responsible for developing, coordinating, and overseeing the implementation of policy, programs, and guidance for the department's suitability program. A suboffice, Personnel Security and Credential Management, is required to conduct oversight and functional program reviews to evaluate compliance and implementation of VA's personnel suitability program requirements of VA Handbook 0710, *Personnel Security and Suitability Program*.[25] Another suboffice, Personnel Security Adjudication Center, is responsible for processing and adjudicating the background investigations for all VA contractors.

All three VA administrations—the Veterans Health Administration (VHA), Veterans Benefits Administration, and National Cemetery Administration—are required to establish a personnel security program manager to coordinate departmental regulations and policies with those of the overall personnel security and suitability program.[26] Personnel security specialists are responsible for determining the suitability and security eligibility of employees and contractors for entry into and retention in sensitive and nonsensitive positions.

The Office of Acquisition, Logistics, and Construction (OALC) is responsible for directing acquisition, logistics, construction, and leasing functions within VA and ensuring these

[23] Effective September 12, 2018, the position of assistant secretary for operations, security, and preparedness was eliminated. The Office of Operations, Security, and Preparedness and its associated functions were reassigned to the assistant secretary for human resources and administration. For consistency, this office is referred to as HRA/OSP throughout the report.

[24] VA Directive 0710.

[25] VA Handbook 0710. The handbook specifies requirements for (a) time frames to complete fingerprint checks, (b) initiation and adjudication of background investigations, (c) uploading investigation documentation into an employee's personnel file, and (d) updating data systems with relevant information.

[26] VA Handbook 0710.

activities comply with all applicable laws and policies. The principal executive director of OALC is also the chief acquisition officer for the department. Within OALC, the Office of Acquisition and Logistics is responsible for acquisition program support, procurement policy, systems, and oversight. The executive director of the Office of Acquisition and Logistics is the senior procurement executive for VA and has authority, direction, and control over the VAAR and the VAAM.

The Office of Information and Technology (OIT) is responsible for developing and implementing a department-wide information system security program in accordance with the Federal Information Security Management Act. The information security program is intended to protect information resources and to provide security measures to mitigate or prevent loss, misuse, or unauthorized access to VA information systems. The assistant secretary for OIT is responsible for providing leadership for the department-wide information security program and approving all VA policies and procedures related to information security.

Results and Recommendations

Finding: VA Officials Did Not Follow Requirements to Ensure Contractor Employees Were Properly Vetted

The OIG determined that VA did not comply with executive orders, federal regulations, or VA requirements for vetting contractor employees.[27] The audit team based this determination on its review of 50 service contracts and records for 286 contractor employees.[28] The review found that

- 47 of 50 contract files (94 percent) did not have the required position designation records that established the background investigation requirements for each contracted employee;
- 34 of 50 contracts (68 percent) did not include the required contract language identifying the position risk and sensitivity designation; and
- 215 of the 286 contractor employee records reviewed (about 75 percent) did not have evidence of a completed fingerprint check completed, and 225 of the 286 (about 79 percent) did not have evidence that a background investigation was completed.

These deficiencies occurred because VA has five directives and handbooks that discuss requirements for vetting contractor employees, but they are outdated and include conflicting or inaccurate information regarding roles and responsibilities. While HRA/OSP and OIT are in the process of updating their respective directives and handbooks, HRA/OSP senior officials initially disregarded formal comments on the updated policies' roles and responsibilities from OALC, the VA subject matter experts for acquisition matters. Compounding these issues, OALC issued guidance to VA acquisition professionals directing them to the wrong policies.

By not complying with contractor employee vetting requirements established by executive orders, federal regulations, and department-wide policies, VA has increased the possibility that individuals working for the federal government are unfit to do so and have gained access to VA facilities, information, or information systems. Unvetted contractor employees may increase risks to the health, safety, and well-being of veterans and VA employees, as well as the efficiency and integrity of VA services, government property, and information. For example, the OIG team evaluated a contract for security guards at the St. Cloud VA Medical Center. This

[27] Exec. Order No. 13764; 5 C.F.R. § 731; VA Directive 0710; VA Handbook 0710.

[28] Appendix A lists the 50 contracts the team reviewed and summarizes its findings. Even though the VA handbook does not explicitly require that a roster of contractor employees be maintained in the contract file, 17 of the 50 contracts reviewed had a roster with a total of 286 contractor employees. The team did not evaluate whether contractor employees from the remaining 33 contracts were vetted because the contract files did not include rosters of contractor employees.

contract included 73 of the 286 contractor employees that the team reviewed. The team determined that the St. Cloud officials did not vet any of the 73 contracted security guards and found that 38 of them (about 52 percent) had criminal records.

The finding is based on the following determinations:

- VA did not comply with executive orders, federal regulations, or its own requirements.
- VA policies did not effectively communicate requirements to the department.
- Unvetted contractor employees increase risks to VA employees and veterans.

What the OIG Did

The audit team reviewed a judgmental selection of 50 service contracts issued between January 1 and December 31, 2020, that required contractor employees to access VA facilities or information. The 50 service contracts were selected based on the OIG team's assessment of the potential risks to veterans and information systems. The service contracts were awarded by officials from VHA, the Veterans Benefits Administration, the National Cemetery Administration, the Strategic Acquisition Center, and the Technology Acquisition Center. The team reviewed the files for each of the selected contracts to obtain the contract and position designation record. The team also reviewed the contracts to determine whether the appropriate risk and sensitivity designation requirements were included.

The audit team obtained rosters of contractor employees from the contract files or acquisition workforce officials. Then, by searching VA-CABS, the team determined whether VA officials conducted the required fingerprint check and background investigation. The team also reviewed documents from VA officials, including emails generated by personnel security specialists.

Finally, the team visited the St. Cloud VA Medical Center to follow up on a hotline allegation related to contractor employee vetting. The team interviewed facility officials and analyzed documents related to contractor performance and vetting actions. The team also conducted a public criminal records review of contractor employees at the St. Cloud VA Medical Center. Appendix B details the audit scope and methodology.

VA Did Not Comply with Executive Orders, Federal Regulations, or VA Requirements

VA officials did not comply with executive orders, federal regulations, or VA's policies for vetting contractor employees. The audit team reviewed 50 contracts to evaluate compliance with the regulations and policies and found high rates of noncompliance. According to federal regulations and VA policies, VA officials must take three key steps to properly vet contractor

employees.[29] As seen in figure 2, VA officials must (1) use the PDT to determine the position's risk and sensitivity levels, (2) ensure appropriate language is included in the contract indicating the results from the PDT, and (3) ensure fingerprint checks and background investigations are conducted, and evaluate and adjudicate the results.

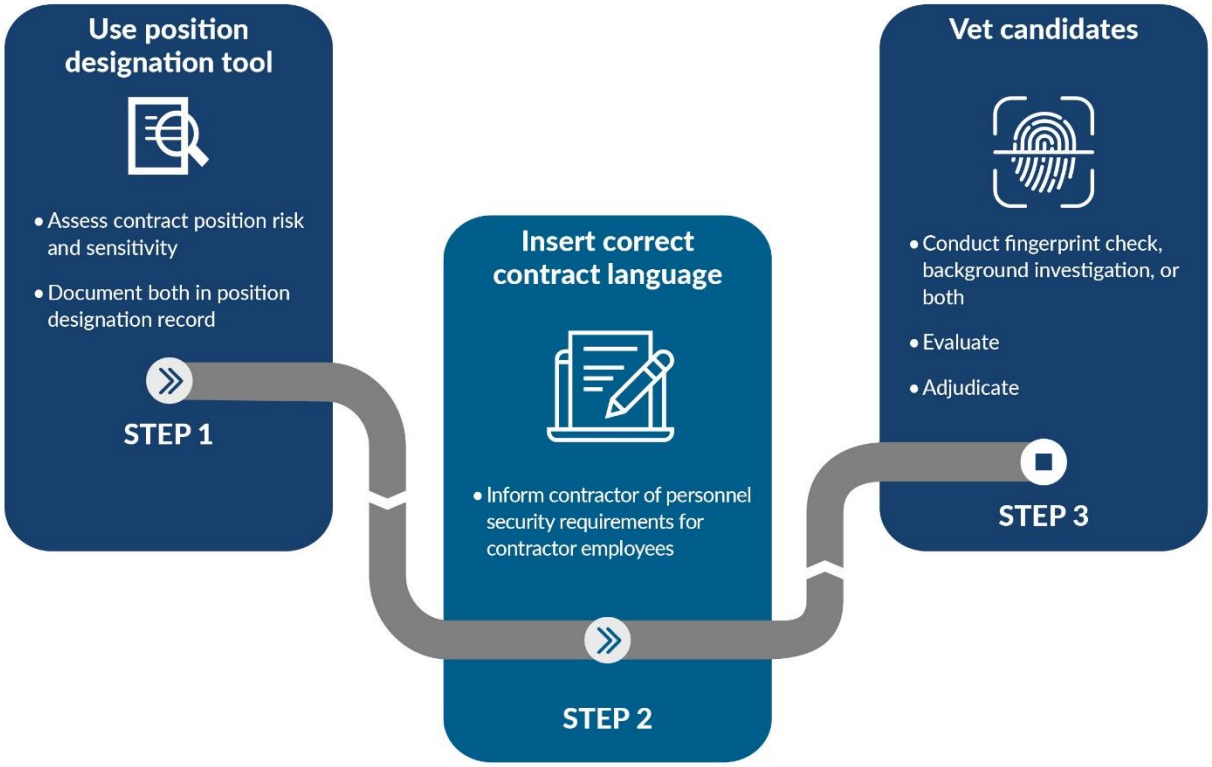


Figure 2. *Key steps in the contractor employee vetting process.*
Source: VA OIG analysis of VA Handbook 0710.

Position Risk and Sensitivity Determinations Were Not Maintained

VA officials did not maintain position risk and sensitivity determinations for contractor employees in accordance with VA policies. For contractor employees, the position risk and sensitivity levels are based on the terms and conditions of the contract.[30] Personnel security specialists are required to work with VA officials to use the PDT to determine each contract's position risk and sensitivity level.[31] The PDT generates a document referred to as the position designation record, which states the position risk, sensitivity level, and background investigation requirements for each position. According to VA policies, the servicing human resource offices or the contracting officer representative is required to maintain a copy of the position designation

[29] 5 C.F.R. § 731.101; 5 C.F.R. § 731.106; Exec. Order No. 13764; VA Directive 0710.
[30] VA Directive 0710; VA Handbook 0710.
[31] VA Handbook 0710.

record for each contract position.[32] Furthermore, pursuant to the Federal Acquisition Regulation, contract files should contain copies of the security requirements, which would include the position designation record.[33] Of the 50 contracts reviewed, 47 (94 percent) did not include the required position designation record, which establishes the risk, sensitivity level, and background investigation requirements for each contracted employee's position.

Contracts Did Not Include Required Language to Communicate Vetting Requirements to Contractors

VA officials did not ensure the appropriate language was included in contracts to indicate the vetting requirements to the contractors. VA policies state that contract language must accurately reflect VA personnel security policies and indicate the position risk and sensitivity levels.[34] VA organizations requiring a contract to accomplish their mission generate the contract requirements, which are submitted to the contracting office as part of an acquisition package. A VA acquisition planning guide reminds the VA activities to define personnel security requirements before sending the acquisition package to the contracting office. Contracting officers are responsible for safeguarding the interests of the United States in its contractual relationships and complying with all laws, executive orders, and regulations before awarding a contract.[35] Therefore, there is a shared responsibility between the VA organization requiring the contract and the contracting officer to ensure that the required language is included in the contract.

The audit team determined that 34 of 50 contracts (68 percent) did not include language as required to accurately reflect VA personnel security policies or indicate the position risk and sensitivity levels.[36] For example, five of the 34 noncompliant contracts were for childcare services, which must include requirements for criminal history background checks in accordance with federal law, acquisition regulation, and agency policy.[37] Specifically, the Federal Acquisition Regulation requires contractor employees that interact with children to undergo fingerprinting and a childcare criminal history background check, as required by law.[38] Furthermore, the VAAR requires contracts for childcare services to include a specific clause

[32] VA Handbook 0710. Contracting officers can delegate, in writing, their authority to perform certain contract administration duties to a designated contracting officer's representative. This authority and the required duties must be detailed in a delegation memorandum.

[33] FAR 4.803.

[34] VA Directive 0710; VA Handbook 0710.

[35] FAR 1.602.

[36] The audit team used a conservative approach to evaluate whether contracts included required contract language. Specifically, the team accepted language that did not explicitly state the risk or sensitivity levels but instead stated the level of background investigation required, which implied the associated risk or sensitivity level.

[37] FAR 37.103; 34 U.S.C. § 20351; VA Handbook 0710.

[38] 34 U.S.C. § 20351; FAR 37.103.

notifying contractors of the requirement for background checks pursuant to federal law.[39] However, the team found that none of the five contracts had the necessary contract language, and only one of the five contracts had the required contract clause. These omissions could have led to unvetted contractor employees working with children.

Contractor Employees Were Not Properly Vetted

VA officials did not comply with federal regulations, executive orders, and VA policies that require officials to ensure all contractor employees are fingerprinted and, as applicable, undergo a background investigation.[40] To determine whether VA properly vetted contractor employees, the audit team obtained a list of 286 contractor employees.[41] The audit team reviewed VA-CABS looking for evidence of each contractor employee's fingerprint check and background investigation.

Of the records for the 286 contractor employees reviewed, the audit team determined that 215 of the 286 contractor employees (about 75 percent) did not have evidence of completed fingerprint checks. Further, of the 286 contractor employees' records, 225 (about 79 percent) did not have evidence of completed background investigations, as shown in figure 3.

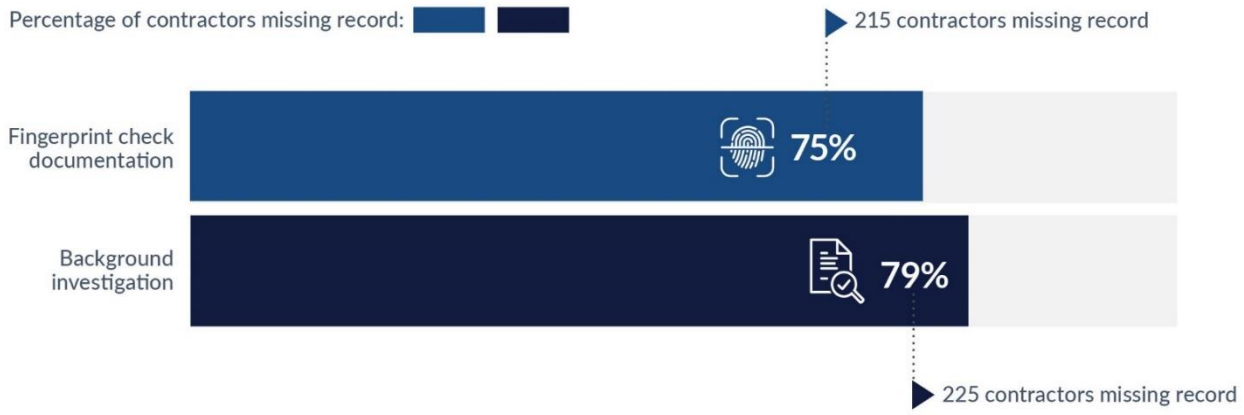


Figure 3. *Contractor employees' fingerprint checks and background investigation records were missing for most of the 286 contractors reviewed.*

Source: VA OIG analysis of 17 contracts awarded from January 1 through December 31, 2020.

[39] VAAR 852.237-73, "Crime Control Act–Requirement for Background Checks."

[40] 5 C.F.R. § 731; VA Directive 0710; VA Handbook 0710; Exec. Order No. 13764.

[41] Even though federal and VA acquisition policies do not explicitly require that a roster of contractor employees be maintained in the contract file, 17 of the 50 contracts reviewed had a roster with a total of 286 contractor employees. The team did not evaluate whether contractor employees from the remaining 33 contracts were vetted because the contract files did not include rosters of contractor employees.

For those contractor employees who had evidence of a fingerprint check or background investigation, the team could not determine whether the appropriate level of investigation was completed when there was no position designation record in the contract file.

VA's Policies Did Not Effectively Communicate Requirements

VA's policies did not effectively communicate requirements to ensure VA staff complied with federal regulations and executive orders. VA's five directives and handbooks that set requirements for vetting contractor employees are outdated, conflicting, and include inaccurate roles and responsibilities. While HRA/OSP and OIT are in the process of updating their respective directives and handbooks, HRA/OSP initially disregarded formal comments on its updated policies' roles and responsibilities from OALC, the subject matter experts for VA acquisition matters. Compounding these issues, OALC issued guidance to VA acquisition professionals directing them to the wrong policies.

VA Directives and Handbooks for Vetting Contractor Employees Are Outdated, Conflicting, and Inaccurate

The five directives and handbooks that discuss vetting contractor employees are outdated, conflicting, and inaccurate. The policies also include unclear guidance and conflicting and inaccurate roles and responsibilities for vetting contractor employees. VA requires policy owners to update their policies at least every five years. In addition, VA policy states that policy authors must ensure new documents do not duplicate or conflict with existing policy, procedures, or guidance.[42]

Outdated Policies

HRA/OSP and OIT's policies are outdated, including two policies which have not been updated since 2010. During that time, the federal requirements for vetting employees and identification standards have been updated multiple times, including an executive order that amended the Civil Service Rules for suitability, fitness, and credentialing in 2017.[43]

Update efforts have so far been unsuccessful. For example, OIT officials stated that they have tried to update VA Handbook 6500.6, *Contract Security*, five times since it was issued in 2010. However, the officials stated that the updates were not published after receiving comments from the department. Most recently, OIT officials stated that in 2021 they received comments during the policy review process that made necessary an extensive rewrite to an appendix. The rewrite, an OIT reorganization, and updates to other related policies contributed to not publishing the updated handbook. As of March 2023, the OIT officials stated that they were in the process of

[42] VA Handbook 0999, *Enterprise Directives Management (EDM) Procedures*, August 1, 2019.

[43] Exec. Order No. 13764.

updating the handbook again. In addition, HRA/OSP officials stated they have been unable to publish updates to VA Handbooks and VA Directives 0710 and 0735 because officials from VHA did not concur with the updates. Table 1 lists the directives and handbooks that include requirements for vetting contractors and the date each was issued.

Table 1. Directives and Handbooks with Contractor Vetting Requirements

Directive/Handbook	Title	Date	Responsible office
VA Directive 0710	Personnel Security and Suitability Program	June 4, 2010	HRA/OSP
VA Handbook 0710	Personnel Security and Suitability Program	May 2, 2016	HRA/OSP
VA Directive 0735	Homeland Security Presidential Directive 12 (HSPD-12) Program	October 26, 2015	HRA/OSP
VA Handbook 0735	Homeland Security Presidential Directive 12 (HSPD-12) Program	March 24, 2014	HRA/OSP
VA Handbook 6500.6	Contract Security	March 12, 2010	OIT

Source: VA OIG analysis of VA directives and handbooks.

Conflicting Requirements

The five directives and handbooks include several conflicting requirements for vetting contractor employees. For example, VA Handbook 0735 defines policies for verifying the identity of VA employees and contractors before issuing identity verification cards. VA uses three credentials for identity verification, and each has defined vetting requirements: a personal identity verification card, a nonpersonal identity verification card, and a flash badge.[44] The handbook states that flash badges can be issued to contractors who just need physical access to facilities and require only a photo identification to verify the applicants' identity.[45] However, VA Directive and Handbook 0710 state that all new contractor employees who are exempt from a background investigation must have, at a minimum, a fingerprint criminal history check.[46] Therefore, the requirements for issuing credentials to contractors in VA Handbook 0735 conflict with the policies for vetting contractors in VA Directive and Handbook 0710.

[44] VA Handbook 0735. Personal identity verification cards are issued to individuals requiring access to VA facilities and information systems for a period of more than 180 days in a calendar year, while nonpersonal identity verification cards are issued for the same access, but for a period of 180 days or less in a calendar year. Flash badges allow individuals access to common areas at VA facilities, but do not allow access to restricted areas or VA information systems.

[45] VA Handbook 0735.

[46] VA Directive 0710; VA Handbook 0710.

Inaccurate Guidance

In addition, VA Handbook 6500.6 includes guidance for vetting contractor employees that is inaccurate because it does not comply with federal and VA personnel security requirements. The executive order and VA policies governing the personnel security and suitability program state that contractors must be vetted if they require access to VA facilities, information, or information systems.[47] VA Handbook 6500.6 is titled "contract security," which is misleading because the purpose of the handbook is to define VA's information security program. When VA officials search for security policies related to contractor employees, the title of VA Handbook 6500.6 could falsely give the impression the handbook encompasses all VA security procedures for contractor employees, which it does not. Further, appendix A of the handbook includes a checklist that must be completed for all information technology service acquisitions to determine the necessary security and privacy controls. The checklist incorrectly states that if a contractor employee does not require access to a VA system or information, indicating the employee only requires access to VA facilities, VA security policies do not apply. However, VA security policies apply to all VA contractor employees, including employees that only require access to VA facilities. Therefore, if a VA official relies solely on VA Handbook 6500.6 to evaluate whether a contractor employee requires vetting, the official may incorrectly exempt from vetting a contractor who only requires physical access to a VA facility. Figure 4 shows an excerpt of the inaccurate checklist.

4.	Will the personnel perform a function that requires access to a VA system or VA sensitive information (e.g., system administrator privileged access to a VA system, or contractor systems or processes that utilize VA sensitive information)? NOTE: See 3.a. under PROCEDURES regarding contracts and agreements concerning medical treatment for Veterans. If the answer above is no, then proceed to the next question. If yes, then VA security policies apply. Contracting Officials need to work with the Program Manager or (procurement requestor), COTR, PO, and ISO to: i. Include the appropriate risk designation of the contractors based on the PDAT determination.	Yes ☐ No ☐

Figure 4. *Question 4 from appendix A, VA Handbook 6500.6.*

Source: VA Handbook 6500.6, Contract Security, March 12, 2010.

Note: The following terms are abbreviated in figure 4: COTR— contracting officer's technical representative; PO—privacy officers; ISO—information security officers; PDAT—position designation automated tool. The VA policies use PDAT and PDT interchangeably for the tool that identifies the position risk and sensitivity levels.

[47] Exec. Order 13764; VA Directive 0710; VA Handbook 0735.

To correct the inaccuracies, OIT should update VA Handbook 6500.6 by changing the title of the handbook and removing personnel security steps that should only be discussed in VA Directive and Handbook 0710.

Unclear Guidance

VA Directive 0710 and VA Handbook 0710 are unclear on what language should be included in contracts to communicate the requirements for vetting contractor employees. The VA directive and handbook state that officials must ensure "appropriate language" is included in applicable contracts that accurately reflects the requirements of VA Directive 0710 and other applicable directives, yet they do not define or provide examples of appropriate language.[48] They further indicate that the contract's statement of work must be reviewed using the PDT and given the appropriate position risk and sensitivity level designation, yet they do not specifically require contracts to state what level of vetting is required for the contract (fingerprint check or background investigation).[49] The audit team interpreted the requirement for contract language to include the position risk and sensitivity levels and a reference to VA Directive 0710. Lacking clear guidance and standard language to include in contracts, VA officials used inconsistent language—some of which did not comply with the directive or the handbook—to communicate the vetting requirements to contractors.

Example 1 presents language in one contract reviewed that does not comply with federal or VA policies, whereas example 2 shows language that includes the required elements.

Example 1

Network Contracting Office 23 awarded a blanket purchase agreement for unarmed security services to support Veterans Integrated Service Network 23 facilities. The agreement stated that contractor employees shall not have criminal records. However, the language in the agreement did not state the position risk level, as required, and incorrectly identified the position sensitivity as "incidental access," which is not one of the federal sensitivity designations.[50] Furthermore, the agreement did not reference VA Directive 0710, as required. Instead, it incorrectly referenced VA Directive 6500.6. Figure 5 shows the incorrect contract language used.

[48] VA Directive 0710; VA Handbook 0710.

[49] Federal acquisition regulation states that contract requirements can be included in a statement of work, a performance work statement, or a statement of objectives.

[50] Sensitivity designation categories include noncritical sensitive, critical sensitive, and special sensitive.

15. **Contractor Personnel Security Requirements:** No access to VA network (s) is required or needed.

a. Position Sensitivity: The position sensitivity has been designated as Incidental Access. Contractor employees and/or agents will not be given access to VA systems or data.
b. Background Investigation: The level of background investigation shall be commensurate with the required level of access and National Agency Check with Written Inquiries. Security Requirements: VA Directive 6500.6, Appendix C, paragraph 1, 2, 6, 7, 9 Appendix D.

Figure 5. *Excerpt of Veterans Integrated Service Network 23 security services blanket purchase agreement.*

Source: Network Contracting Office 23 contract number 36C2630A0021.

Example 2

Technology Acquisition Center officials awarded a $2.9 million contract for fiscal and auditing support services for the Supportive Services for Veteran Families Program. The contract outlined the fingerprinting and background investigation requirements and informed the contractor of the forms needed to vet its employees. Figure 6 shows the contract language used.

6.1.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☐	☐	☒
5.2	☐	☐	☒
5.3	☐	☐	☒
5.4	☐	☐	☒
5.5	☐	☐	☒
5.6	☐	☐	☒
5.7	☐	☐	☒
5.8	☐	☐	☒

The Tasks identified above, and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

Figure 6. *Excerpt of Supportive Services for Veteran Families Program contract.*

Source: Technology Acquisition Center contract number 36C10B20F0060.

Conflicting and Inaccurate Roles and Responsibilities

Finally, the directives and handbooks include several conflicting and inaccurate roles and responsibilities for vetting contractor employees. During the acquisition process, the VA organization requiring the contract prepares a statement of work explaining the position description of each contract employee. Drafting the statement of work is the responsibility of the VA organization because its staff know most about the services required. The VA organization submits this as part of an acquisition package to the contracting office. During the process, the contracting office can provide assistance or guidance to the VA organization from an acquisition perspective—for example, guidance on ways to enhance competition—but it does not write the statement of work. To help the VA organization develop its acquisition package, OALC issued a VA acquisition planning guide.[51] The guide includes a checklist directing the VA organizations to, among other things, define personnel security requirements before sending the acquisition package to the contracting office. Figure 7 depicts the process to develop an acquisition package.

[51] VA Acquisition Academy, *Acquisition Planning Guide*, Version 2, Release 1, n.d.

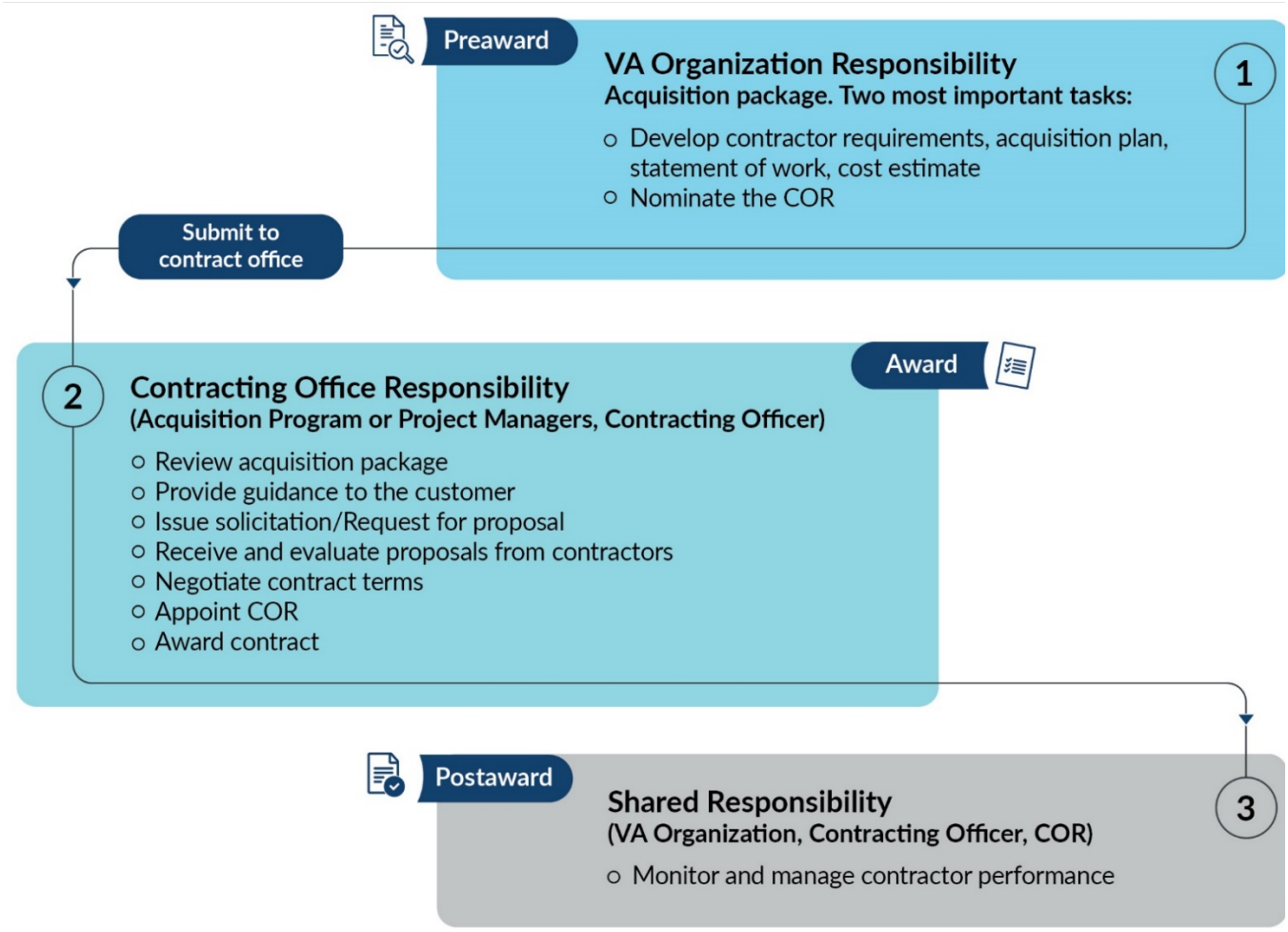


Figure 7. *Planning and award phases of the acquisition lifecycle.*
Source: VA OIG analysis of VA acquisition planning guide.

While in one place VA Handbook 0710 states that only human resources specialists and personnel security specialists are authorized to determine position risk and sensitivity levels using the PDT, elsewhere the handbook and VA Directive 0710 assign this responsibility to several other officials:

- OALC
- Program managers[52]
- Contracting officers

[52] The term program manager has multiple meanings. When referring to a program manager along with contracting personnel, the audit team interpreted the role as the acquisition program manager, who is part of the certified acquisition workforce. However, the customer requiring a contract may also have program managers who are responsible for programs in their respective career field.

- Contracting officer's technical representatives
- Contracting officer's representatives

Assigning use of the PDT to contracting officials not only contradicts guidance elsewhere in VA Handbook 0710 limiting this authority to human resources specialists and personnel security specialists, but also incorrectly designates responsibility to define the personnel security requirements in statements of work to OALC, program managers, contracting officers, and contracting officer's representatives.

VA Disregarded Input from Subject Matter Experts When Updating Contractor Vetting Policies

While HRA/OSP is in the process of updating VA directives and handbooks 0710 and 0735, the draft updates the OIG team obtained did not resolve conflicting roles and responsibilities. One reason was that HRA/OSP senior officials initially disregarded comments on the proposed updates from OALC, the VA subject matter experts on acquisition. To coordinate draft policies, VA uses the Veterans Affairs Integrated Enterprise Workflow Solution (VIEWS) system to obtain concurrence and to document management comments from subject matter experts and decision-makers throughout VA. VA policy states that all appropriate VA organizations and staff offices must concur with new policies before VA publishes them.[53]

During the update process, OALC officials provided HRA/OSP comments on the accuracy of the roles and responsibilities for vetting contractor employees. OALC's comments were labeled as critical comments that would prevent the agency from concurring with the updated policy. In particular, OALC officials indicated they should be responsible for developing and issuing VA acquisition policy, including contract clauses, and should not be responsible for performing personnel security duties. OALC's comments emphasized that the VA organization requiring the contract should be responsible for performing personnel security responsibilities, including using the PDT to identify risk and sensitivity levels, and for incorporating personnel security language into the contract statement of work.

The documentation provided to the audit team indicated that HRA/OSP senior officials updated the draft policies based on OALC's comments and resolved OALC's concerns in June 2022. However, the updated drafts of the directive and handbook that HRA/OSP officials provided the audit team in March 2023 still included the inaccurate and conflicting roles and responsibilities that OALC stated were critical concerns. Table 2 provides a side-by-side comparison of the existing policies and the drafts provided to the audit team.

[53] VA Directive 0999, *Enterprise Directives Management (EDM)*, October 9, 2018; VA Handbook 0999.

Table 2. Contractor Vetting Roles and Responsibilities in Existing Policy and Draft Updates

Existing policy	Concerns	Draft updates obtained by the OIG in March 2023
VA Handbook 0710 **Office of Acquisition, Logistics, and Construction** will: 1. Ensure the SOW [statement of work] (or other defining documentation related to the contract) be reviewed using the PDT and given the appropriate position risk and sensitivity level designation. 2. Ensure a fingerprint check is completed on contractor employees and adjudicated at local facilities by a trained adjudicator.	VA organizations requiring contracts should be responsible for using the PDT to define the personnel security requirements in the SOW, instead of OALC officials. OALC officials should be responsible for developing and issuing VA acquisition policy, including contract clauses, instead of performing personnel security duties, such as ensuring fingerprint checks are completed and adjudicated.	VA Directive 0710 **Principal Executive Director for Office of Acquisition, Logistics, and Construction** shall, in addition to Para c above: 1. Ensure all defining documentation related to the contract be reviewed using the PDT and given the appropriate position risk and sensitivity level designation. 2. Ensure a fingerprint check is completed on all new contractor employees and adjudicated by a trained adjudicator prior to performing work under a VA contract.
VA Directive 0710 The PDAT will be used by Contracting Officers and **Contracting Officer Technical Representative** to appropriately designate the statement of work or other written description of the assignment, with the proper risk or sensitivity level for the contract employees.	The SOW is written by VA organizations requiring a contract. Therefore, the SOW should include the risk and sensitivity levels for contractor employees before the SOW is provided to the contracting office.	VA Directive 0710 The PDAT must be used by Contracting Officers and **Contracting Officer Representatives** (CO/COR) to appropriately designate the Statement of Work or other written description of the assignment, with the proper risk or sensitivity level for contractors.

Source: VA OIG analysis of existing and drafted VA Directive and Handbook 0710 furnished by HRA/OSP.

As shown in the table, as of March 2023, the draft handbook and directive still incorrectly state that OALC, the contracting officer, and the contracting officer's representative must use the PDT to appropriately designate the statement of work with the proper risk and sensitivity level for contractor employees. By ignoring subject matter experts' guidance on these roles and responsibilities, senior officials at HRA/OSP misinterpreted the roles of the acquisition workforce.

In July 2023, the audit team communicated its concerns with the draft policies to an HRA/OSP official, who took corrective action. The official acknowledged that HRA/OSP officials misinterpreted the comments from OALC. The official subsequently stated that HRA/OSP reopened discussions with OALC about the comments and updated the draft policies

accordingly. The HRA/OSP official provided the audit team updated drafts of VA Directive and Handbook 0710 that appropriately assign OALC responsibility for establishing acquisition policy, while assigning responsibility for using the PDT to the VA organizations requesting a contract.

VA Issued Inadequate Acquisition Guidance

While the Federal Acquisition Regulation does not provide specific guidance for vetting contractor employees, it states that no contract shall be entered into unless the contracting officer ensures that all requirements of law, executive orders, regulations, and all applicable procedures, including clearances and approvals, have been met.[54] These include the federal regulations and executive orders for personnel security and contractor employee vetting.[55] In addition, the Federal Acquisition Regulation requires the contract statement of work to define personnel security requirements.[56] To assist contracting officers with compliance, the Office of Acquisition and Logistics issues VA acquisition policies, such as the VAAR and the VAAM, along with guidance and information to VA acquisition professionals. However, the Office of Acquisition and Logistics issued guidance to VA acquisition professionals directing them to the wrong policies for contractor employee vetting, thereby limiting their ability to comply with the applicable laws and regulations.

The VAAR includes inadequate guidance that does not direct the acquisition professionals to federal and VA requirements for vetting all contractor employees. Instead, it includes requirements for issuing contractors identity verification cards that grant the employees access to VA facilities or information systems, requirements for information security, and requirements for conducting background checks on contractors who work in childcare services.[57] However, it does not include requirements for vetting all contractor employees.

Supplementing the VAAR is the VAAM. The VAAM also does not include procedures or guidance for vetting contractor employees, such as the use of the position designation tool or contract language requirements.[58] In 2021, the VAAM referenced VA Directive 0710 in a section discussing personnel identity verification cards, rather than personnel security procedures. Specifically, the VAAM incorrectly directed the acquisition workforce to follow the procedures in VA Directive 0710 to ensure compliance with Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and

[54] FAR 1.602-1(b).

[55] 5 C.F.R. § 731; Exec. Order No. 13764.

[56] FAR 8.405-2.

[57] VAAR 804.1303; VAAR 804.1970; VAAR 837.403-70; and VAAR 852.237-73.

[58] When the Office of Acquisition and Logistics updates the VAAM, the VAAM does not include the version or date it was updated. The audit team downloaded and reviewed versions of the VAAM in 2021 and 2023 to evaluate requirements for vetting contractor employees.

Contractors." However, VA Directive and Handbook 0735 implement the Presidential Directive, not VA Directive 0710. Subsequently, the Office of Acquisition and Logistics removed the reference to VA Directive 0710 from the VAAM. Therefore, the VAAM does not direct the acquisition professionals to the requirements for vetting contractor employees.

Instead of directing VA acquisition professionals to the requirements for vetting contractor employees, the Office of Acquisition and Logistics issued multiple policies and guidance incorrectly directing VA acquisition professionals to VA Handbook 6500.6, *Contract Security*. For example, the Office of Acquisition and Logistics issued a policy flash that directed the use of VA Handbook 6500.6 for all service contracts.[59] The policy flash incorrectly states that the handbook establishes VA procedures, responsibilities, and processes for implementing security policy as appropriate in VA acquisitions for services. The VAAM also directs contracting officer's representatives to the handbook for their roles and responsibilities. The acquisition planning guide, too, includes a checklist that directs VA officials to the handbook. However, as previously stated, VA Handbook 6500.6 includes inaccurate guidance for vetting contractor employees, giving the impression that contractor employee vetting procedures only apply when contractors require access to VA information or information systems. Therefore, by directing VA acquisition professionals to VA Handbook 6500.6, instead of citing VA Directive and Handbook 0710, the Office of Acquisition and Logistics issued inadequate guidance, directing VA acquisition professionals to the wrong policies for contractor employee vetting. To address the inadequate guidance, the Office of Acquisition and Logistics should update the VAAR and VAAM to direct VA acquisition professionals to the correct guidance for vetting contractor employees and should rescind or update the policy flash.

Unvetted Contractor Employees Increase Risks to VA Employees and Veterans

By not complying with federal and VA contractor employee vetting requirements, VA increased the possibility that individuals working for the federal government are unfit to do so and may have gained access to VA facilities, information, or information systems. During the audit, the VA OIG received a hotline complaint that emphasized the importance of vetting contractor employees.

In May 2021, the VA OIG received a hotline allegation regarding a contract for unarmed security guards at the St. Cloud VA Medical Center. The complainant reported concerns about insufficient vetting of contractor employees, who then exhibited unethical behavior while working for VA, including sexual harassment and racist and sexist comments. Therefore, the audit team reviewed the allegation and incorporated the contract into its review.

[59] Acquisition Policy Flash 16-13. Acquisition policy flashes are used to communicate information that has the potential to impact day-to-day procurement operations within VA.

In May 2020, VHA issued the contract to obtain unarmed security guard services. The security guards could be tasked with duties such as observation, COVID-19 screening, building and grounds surveillance, traffic control, the discovery and detention of unauthorized individuals, and protective functions, if necessary, at several locations in Veterans Integrated Service Network 23, including the St. Cloud VA Medical Center in Minnesota.[60] The contractor provided services between May 1, 2020, and September 30, 2021. The team evaluated the contract to determine whether it included contractor employee vetting requirements and evaluated whether the contractor employees were vetted in accordance with federal and VA policies.

The audit team determined that the contract included language for vetting contractor employees that did not comply with federal and VA policies. According to federal regulations, public safety and law enforcement positions demand a significant degree of public trust and should be designated at moderate or high risk levels, which would result in more stringent vetting requirements.[61] Therefore, the contractor employees should have been required to undergo background investigations. The contract appropriately stated that the contractor employees must not have criminal records. In addition, federal regulations state that only the government's investigative service provider is authorized to conduct background investigations for the government.[62]

However, the contract inappropriately directed the contractor to conduct its own background checks, and the contractor was not required to provide the results of the checks to the government unless requested. Figure 8 is an excerpt of the contract requirements that instructed the contractor to perform its own background checks.

a) Contractor employees providing services under this contract shall not have any criminal record. The Contractor shall conduct their own background checks on their employees prior to ensure suitability of performance under this contract prior to the employee's start date. Upon request, the Contractor shall provide documentation to the Contracting Officer or Contracting Officer's Representative (COR) of these completed background check. All Contractor personnel who will provide unarmed security guard services shall obtain contractor badges from the PIV office (VA Police Department) and shall always display/wear the Contractor's badge. There could be risk of exposure to COVID 19

Figure 8. *Excerpt of contract requirements.*
Source: Contract 36C26320A0021.

[60] The security guard contract included multiple locations in VA Integrated Service Network 23. However, the audit team only focused on whether contractors were vetted at the St. Cloud VA Medical Center because the hotline specifically identified concerns with that location.

[61] 5 C.F.R. § 731.106. Based on the responsibilities for contracted security guards, the audit team determined the positions relate to public safety.

[62] Exec. Order No. 13764; 5 C.F.R. § 731.104.

To determine whether the contractor employees were vetted in accordance with federal and VA requirements, the audit team obtained a roster of the 73 contractor employees that worked as security guards at the St. Cloud VA Medical Center. The team reviewed VA-CABS to determine whether the contractor employees had fingerprint checks or background investigations performed by the government and documented in the system. VA-CABS did not have records for any of the 73 contractor employees. The audit team then used a publicly available Minnesota state website to determine if the contractor employees had criminal records. Based on the public records search, the team determined that 38 of 73 contractor employees had criminal records before or during the contract's period of performance.[63] The records of these 38 contractor employees included arrests and convictions ranging from petty misdemeanors to felonies.[64] For example, some of the criminal records of the contractor employees included

- disorderly conduct,
- domestic abuse,
- physical and sexual assault,
- sexual misconduct,
- felony theft,
- drug sales,
- financial card fraud, and
- terroristic threats.

VA police, St. Cloud officials, and the VA OIG were notified about improper behavior by the unvetted contractor employees throughout the contract's period of performance, including

- stalking female VA and contractor employees,
- sexually harassing and sexually assaulting other employees at the St. Cloud VA Medical Center,
- making racist and sexist comments,
- getting into altercations with other contractor employees that required police intervention,

[63] Publicly available criminal records may not include all offenses. Some criminal records may be sealed from public disclosure. Records pertaining to offenses occurring in other jurisdictions would also be excluded.

[64] Criminal acts fall into two categories: felonies and misdemeanors. Felonies are offenses that may result in prison sentences of more than one year, while misdemeanors carry sentences of one year or less. Although misdemeanors are less serious, they are still considered crimes.

- bragging to coworkers about being in a gang responsible for a stabbing, and
- being arrested for felony discharge of a firearm inside city limits.

Based on the nature of the criminal offenses and the type of conduct reported during the performance of the contract, proper vetting as required may have prevented some of this conduct at the St. Cloud VA Medical Center. The OIG previously published a report with a recommendation for HRA/OSP to reimplement the monitoring program required by VA Handbook 0710 as part of VA's oversight efforts to identify and prevent systemic weaknesses in the personnel suitability program.[65] Therefore, although the audit team identified deficiencies with several VA contracts, this report only recommends that HRA/OSP conduct a compliance inspection at Network 23 due to the nature of the deficiencies identified.

Conclusion

Federal regulations and executive orders establish requirements for vetting government employees and contractors to ensure that people working for or on behalf of the government are loyal to the United States, reliable, trustworthy, and of good character and conduct. The executive order and VA policies require contractor employees to be vetted before being granted access to VA facilities, information, or information systems. When contractors are not vetted in accordance with the federal and VA requirements, they may pose risks to the health and well-being of veterans and VA employees as well as the efficiency and integrity of VA services, government property, and information. The audit team found that VA did not comply with the federal regulations, executive order, and VA policies, and VA's policies did not effectively communicate requirements. Unless VA improves its compliance with federal regulations and executive orders and updates and clarifies its internal policies and procedures for vetting contractor employees, VA may hire other contractor employees who could put employees, veterans, information, and information systems at increased risk.

Recommendations 1–6

Because of the long-standing disagreements between the Office of the Assistant Secretary, Human Resources and Administration/Operations, Security, and Preparedness and the Office of Acquisition, Logistics, and Construction on roles and responsibilities for personnel security, the OIG issued a recommendation to the VA Deputy Secretary to take the following action:

1. Mediate the two offices' collaboration to develop and publish updates to the personnel security policies and procedures for vetting contractor employees to include appropriate roles and responsibilities; standard contract language to

[65] VA OIG, *VA's Governance of Its Personnel Suitability Program for Medical Facilities Continues to Need Improvement*.

communicate the requirements for vetting contractor employees, including whether a fingerprint check or background investigation is required, that can be used across the department; and a requirement that the VA organization requesting a contract provide the position designation record in the acquisition package submitted to the contracting office.

The OIG made a recommendation to the assistant secretary, human resources and administration/operations, security, and preparedness:

2. Perform and document compliance inspections of the procedures for vetting contractor employees and the issuance of VA identification credentials at medical facilities supported by Network Contracting Office 23, including the St. Cloud VA Medical Center.

The OIG made two recommendations to the executive director of the Office of Acquisition and Logistics and senior procurement executive:

3. Update and publish the Veterans Affairs Acquisition Regulation and Veterans Affairs Acquisition Manual to direct the department's acquisition professionals to the correct guidance for vetting contractor employees, which should include VA's personnel security and suitability program policy.
4. Update and publish or rescind Acquisition Policy Flash 16-13, "Use of VA Handbook 6500.6, Appendix A, Checklist for Information Security in VA Service Acquisitions," to ensure VA acquisition professionals understand that VA Handbook 6500.6 is not the only personnel security policy they must comply with.

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

5. Update and publish VA Handbook 6500.6, *Contract Security*, in collaboration with the Office of Acquisition, Logistics, and Construction and the Office of Human Resources and Administration/Operations, Security, and Preparedness, including retitling it to better correspond to its content and removing any personnel security steps that should only be discussed in VA personnel security and suitability program policies.

The OIG recommended that the director of Network Contracting Office 23 do the following:

6. Review the actions of the officials responsible for planning, awarding, and administering contract 36C26320A0021, which included vetting procedures that did not comply with federal or VA policies, and take administrative action if appropriate.

VA Management Comments

The Deputy Secretary agreed with the OIG's finding, concurred in principle with recommendation 1, and concurred with recommendations 2 through 6. The full text of the Deputy Secretary's comments and action plan appears in appendix C.

For recommendation 1, the Deputy Secretary concurred in principle and stated HRA/OSP has established and communicated standardized contractor vetting processes. The Deputy Secretary also stated that contract clauses are in place and that various policies and clauses are continuously reviewed and updated when necessary.

For recommendation 2, the Deputy Secretary responded for the assistant secretary, human resources and administration/operations, security, and preparedness and stated HRA/OSP will perform and document compliance inspections of the contractor employee vetting procedures and issuance of the VA personal identity verification credentials at Network Contracting Office 23 medical facilities, including St. Cloud VA Medical Center. The target completion date for this action is March 31, 2024.

For recommendations 3 and 4, the Deputy Secretary responded for the executive director of the Office of Acquisition and Logistics and senior procurement executive. For recommendation 3, the Deputy Secretary stated OALC will make the appropriate acquisition regulatory guidance for VA contractors in the Veterans Affairs Acquisition Regulation and Veterans Affairs Acquisition Manual after OIT and HRA/OSP finalize updates to their policies and procedures. The target completion date for this action is September 30, 2024. For recommendation 4, OALC rescinded Acquisition Policy Flash 16-13 on October 27, 2023.

For recommendation 5, the Deputy Secretary responded for the assistant secretary for information and technology and stated that the Office of Information Security Information Security Policy is collaborating with the OALC and HRA/OSP to update VA Handbook 6500.6, including the title and removal of all personnel security steps. The target completion date for this action is September 30, 2024.

For recommendation 6, the Deputy Secretary responded for the director of Network Contracting Office 23 and stated the VHA Policy Oversight and Assessment Office completed a review of the contract file and recommended appropriate actions for relevant officials. Further, the office recommended updates for a VHA internal guide to better communicate security-related documentation that must be included in the acquisition package.

OIG Response

The Deputy Secretary concurred in principle with recommendation 1, and although the Deputy Secretary agreed with the recommendation the comments were not fully responsive. The Deputy Secretary's response stated that HRA/OSP has established and communicated standardized contractor vetting processes, and that contract clauses are in place. However, the Deputy

Secretary's comments were not precise as to whether the existing policies and contract clauses were sufficient or whether updates to the policy and clauses were made in response to the recommendation. This recommendation was made to the Deputy Secretary to address the long-standing disagreements between the Office of the Assistant Secretary, Human Resources and Administration/Operations, Security, and Preparedness and the Office of Acquisition, Logistics, and Construction on roles and responsibilities for personnel security. VA's five directives and handbooks that discuss vetting contractor employees are outdated, conflicting, and inaccurate. Further, HRA/OSP initially disregarded OALC comments on proposed changes when updating the VA directive and handbooks. As a result, the OIG believes that it is necessary for the Deputy Secretary to take an active and ongoing role in ensuring HRA/OSP and OALC officials develop and publish the necessary personnel security policy and procedure updates for vetting contractor employees as stated in the recommendation. Accordingly, the recommendation will stay open until the Deputy Secretary demonstrates sufficient progress on the implementation and fulfillment of the recommendation's intent.

The Deputy Secretary reported that corrective actions for recommendations 2, 3, and 5 were in progress and provided estimated completion dates. The planned corrective actions are responsive to the intent of the recommendations. The OIG will monitor VA's progress on its proposed actions and will close recommendations 1, 2, 3, and 5 when documentation has been provided to demonstrate sufficient progress on implementation and fulfillment of the recommendations' intent. The actions taken and documented for recommendations 4 and 6 were fully responsive. The OIG considers both recommendations closed as implemented.

Appendix A: Contracts Reviewed

The audit team reviewed 50 contracts. Table A.1 summarizes whether the contract file had a position designation record, included the correct language, and whether the audit team performed a roster review of the contractor employees.

Table A.1: Summary of Contracts Reviewed

Contract	Contract number	Order number	Contract included position designation record	Contract included correct language	Audit team performed roster review
1	36C10G20A0007	36C10G20F0014			X
2	36C10X19A0015	36C10X20N0048		X	
3	36C10X19D0002	36C10X21N0011		X	
4	36C10X19D0006	36C10X21N0018		X	
5	36C10X21C0008	N/A		X	X
6	36C24118D0091	36C24120N0360		X	
7	36C24119D0032	36C24120N0908			
8	36C24219D0084	36C24220N0434			
9	36C24420A0012	36C24420N0604			X
10	36C24620C0104	N/A			
11	36C24620D0062	36C24621N0126		X	X
12	36C24720A0021	36C24720N0546			
13	36C24720A0021	36C24720N0545			
14	36C24820A0004	36C24820N0332			
15	36C25020C0163	N/A			X
16	36C25021D0007	36C25021N0071			X
17	36C25220C0099	N/A			
18	36C25820C0038	N/A			
19	36C25920C0044	N/A			
20	36C26019D0003	36C26020N0794			X
21	36C26320A0016	36C26320N0646	X		
22	36C26320A0021	Multiple			X
23	36C78618D0032	36C78620N0315			
24	36C78618D0174	36C78621N1004			
25	36C78619D0155	36C78620N0403			

Contract	Contract number	Order number	Contract included position designation record	Contract included correct language	Audit team performed roster review
26	36C78619D0162	36C78620N0502			
27	36C78620C0285	N/A			
28	36C78620D0027	36C78621N0207			
29	36C78621D0016	36C78621N0094			X
30	47QRAA20D008D	36C10D20F0009		X	X
31	47QSHA20D000K	36C10E20F0111		X	X
32	GS-00F-280DA	36C25820F0130			
33	GS-02F-0212X	36C10B20F0074		X	
34	GS-02F-0212X	36C10B20F0173		X	X
35	GS-07F-0174Y	36C26120F0224			
36	GS-07F-167GA	36C78621F0017			
37	GS-10F-227AA	36C10D21F0002	X	X	X
38	GS-21F-0185X	36C24720F0263			X
39	GS-21F-0215W	36C78621F0002			
40	GS-23F-053AA	36C10B20F0060		X	X
41	N/A	36C24920P0373			
42	N/A	36C24920P0416			
43	N/A	36C26121P0049			
44	N/A	36C25620P0781			
45	N/A	36C25620P0788			
46	N/A	36C24620P1084			
47	VA119A-17-D-0020	36C10E20N0092		X	
48	VA119A-17-D-0038	36C10E21N0008		X	X
49	VA119A-17-D-0046	36C10E20N0179		X	
50	VA240-17-A-0004	36C24E20N0182	X	X	X
		Total	**3**	**16**	**17**

Source: VA Office of Inspector General (OIG) analysis of 50 sampled contracts.

Appendix B: Scope and Methodology

Scope

The audit team conducted its work from October 2021 through August 2023. The audit reviewed the process that VA officials used to vet contractor employees. The audit focused on whether VA officials complied with federal regulations, executive orders, and VA policies for vetting contractor employees. The audit team judgmentally selected 50 service contracts issued by the Veterans Health Administration (VHA), Veterans Benefits Administration, National Cemetery Administration, Technology Acquisition Center, and Strategic Acquisition Center. The contracts were issued between January 1, 2020, and December 31, 2020.

Methodology

To achieve the audit objective, the team did the following:

- Identified and reviewed applicable laws, regulations, VA policies, and operating procedures
- Conducted interviews of VA personnel associated with vetting contractor employees
- Solicited information regarding the contractor employee vetting process from various VA offices
- Reviewed and addressed a relevant hotline complaint
- Reviewed the VA Centralized Adjudication Background Investigation System (VA-CABS) to determine whether contractor employees received fingerprint checks or background investigations
- Reviewed public criminal records for contractor employees at the St. Cloud VA Medical Center in Minnesota

The audit team also performed a site visit at the St. Cloud VA Medical Center in February 2022. During the site visit, members of the audit team interviewed management and staff regarding topics related to vetting contractor employees.

Internal Controls

The audit team assessed the internal controls for vetting contractor employees that were significant to the audit objective. This included an assessment of the five internal control components: control environment, risk assessment, control activities, information and

communication, and monitoring.[66] In addition, the team assessed the principles of those internal control components. The team identified internal control deficiencies with one component and two principles.[67]

- Component 3: Control Activities
    - Principle 10: Design control activities. Design of appropriate types of control activities, establishment and review of performance measures and indicators.
    - Principle 12: Implement control activities. Management should implement control activities through policies.

Fraud Assessment

The audit team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the audit objectives, could occur during this audit. The team exercised due diligence in staying alert to any fraud indicators by identifying regulations and procedures related to the audit subject matter to help detect noncompliance or misconduct and completing the Fraud Indicators and Assessment Checklist. The OIG did not identify any instances of fraud during this audit.

Data Reliability

The OIG relied on contract file information from the electronic contract management system. To test for reliability, the OIG checked data elements, such as missing data fields, alphabetic characters in a numeric field, and illogical data relationships, and compared merged data to original data. The OIG concluded that the data were reliable and appropriate to support the findings and recommendations.

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 the findings and conclusions based on audit objectives. The OIG believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

[66] Government Accountability Office, *Standards for Internal Control in the Federal Government,* GAO-14-704G, September 2014.

[67] Since the audit was limited to the internal control components and underlying principles identified, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Appendix C: VA Management Comments

Department of Veterans Affairs

Memorandum

Date:

From: Deputy Secretary (001)

Subject: Office of Inspector General (OIG) Draft Report: Noncompliance with Contractor Employee Vetting Requirements Exposes VA to Risk (2021-03255-AE-0161) (VIEWS 10840358)

To: Director, Office of Communications and Public Affairs (50P)

1. In response to your request, I submit the attached comments for the subject OIG Draft Report.

The OIG removed point of contact information prior to publication.

(Original signed by)

Tanya J. Bradsher

Attachment

Attachment

OIG Draft Report Finding: VA Officials Did Not Follow Requirements to Ensure Contractor Employees Were Properly Vetted.

VA Response: Concur.

Recommendation 1: Mediate the two offices' collaboration to develop and publish updates to the personnel security policies and procedures for vetting contractor employees to include appropriate roles and responsibilities; standard contract language to communicate the requirements for vetting contractor employees, including whether a fingerprint check or background investigation is required, that can be used across the department; and a requirement that the VA organization requesting a contract provide the position designation record in the acquisition package submitted to the contracting office.

VA Response: Concur in Principle. Standardized contractor vetting processes have been established and communicated by HRA/OSP as well as contract clauses for OALC contractors are in place. Various policies and clauses are continuously reviewed and updated in the normal course of business, as necessary.

Recommendation 2: The OIG made a recommendation to the Assistant Secretary, Human Resources and Administration/Operations, Security, and Preparedness:

Perform and document compliance inspections of the procedures for vetting contractor employees and the issuance of VA identification credentials at medical facilities supported by Network Contracting Office 23, including the St. Cloud VA Medical Center.

VA Response: Concur. HRA/OSP will perform and document compliance inspections of the procedures for vetting contractor employees and the issuance of VA personal identity verification credentials at medical facilities supported by Network Contracting Office (NCO) 23, including the St. Cloud VA Medical Center, starting in the first quarter of fiscal year (FY) 2024, and completing in the second quarter of FY 2024, (March 31, 2024).

Additionally, when there is additional standardized guidance from HRA/OSP which is directed to the VA contractors, the Office of Acquisition and Logistics (OAL) will review the guidance in collaboration with HRA/OSP and will add it to the acquisition regulatory guidance in the VA Acquisition Regulation (VAAR) and/or VA Acquisition Manual (VAAM) where appropriate.

Target Completion Date: March 31, 2024

Recommendation 3: The Executive Director of the Office of Acquisition and

Logistics and Senior Procurement Executive: Update and publish the Veterans Affairs Acquisition Regulation and Veterans Affairs Acquisition Manual to direct the departments' acquisition professionals to the correct guidance for vetting contractor employees, which should include VA's personnel security and suitability program policy.

VA Response: Concur. Collaboration is required with the Office of Information and Technology (OIT) to address the response to this recommendation. OAL's response to this recommendation is dependent on updates from OIT and if necessary HRA/OSP. When these updates are finalized and include directives for the VA Contractors, OAL will develop and implement appropriate acquisition regulatory guidance in the VAAR and/or VAAM.

Target Completion Date: September 30, 2024

Recommendation 4: The Executive Director of the Office of Acquisition and

Logistics and Senior Procurement Executive: Update and publish or rescind Acquisition Policy Flash 16-13, "Use of VA Handbook 6500.6, Appendix A, Checklist for Information Security in VA Service Acquisitions," to ensure VA acquisition professionals understand that VA Handbook 6500.6 is not the only personnel security policy they must comply with.

VA Response: Concur. Acquisition Policy Flash 16-13 has been removed. VA considers actions on this recommendation to be complete and asks OIG to consider closure.

Completion Date: October 2023

Recommendation 5: The OIG recommended the Assistant Secretary for Information and Technology take the following action: Update and publish VA Handbook 6500.6, Contract Security, in collaboration with the Office of Acquisition, Logistics, and Construction and the Office of Human Resources and Administration/Operations, Security, and Preparedness, including retitling it to better correspond to its content and removing any personnel security

steps that should only be discussed in VA personnel security and suitability program policies.

VA Response: Concur. OIT, Office of Information Security, Information Security Policy (ISP) is responsible for the development and maintenance of VA Handbook 6500.6, Contract Security. ISP is collaborating with subject matter experts from OALC and HRA/OSP, to update VA Handbook 6500.6. ISP is currently drafting an updated VA Handbook 6500.6 and will ensure the revision is retitled and has all personnel security steps removed, with an anticipated completion and publication date of September 30, 2024.

Target Completion Date: September 30, 2024

Recommendation 6: The OIG recommended that the director of Network Contracting Office 23 do the following: Review the actions of the officials responsible for planning, awarding, and administering contract 36C26320A0021, which included vetting procedures that did not comply with federal or VA policies, and take administrative action if appropriate.

VA Response: Concur. The VHA Procurement Policy Oversight and Assessment Office completed its review of the contract file and has recommended appropriate actions with respect to relevant officials and has recommended updates be made to VHA's Customer Reference Guide to better communicate security-related documentation submittals to be included with an acquisition package. VA considers actions on this recommendation to be complete and asks OIG to consider closure.

Completion Date: October 2023

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	Christopher Bowers, Director Christopher Kinney David Kolberg Heather Robinson Judith Sterne Steven Walton Scott Wetzel Danita Young
Other Contributors	Victoria M. Eatherton Juliana Figueiredo Allison Tarmann William Tettemer

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

Non VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
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.vaoig.gov.