US DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Review of Contracted Backup Services for the Veterans Crisis Line

Review	23-03464-146	September 1, 2026

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

OUR MISSION

To conduct independent oversight of the Department of Veterans Affairs that combats fraud, waste, and abuse and improves the effectiveness and efficiency of programs and operations that provide for the health and welfare of veterans, their families, caregivers, and survivors.

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's (OIG) healthcare inspections directorate, during a previous review of the Veterans Crisis Line's (VCL) implementation of the National Suicide Prevention Hotline three-digit dialing code (988 press 1, launched in 2022), raised concerns that VA may have paid for contracted call responder backup services that were not provided for more than a year.[1] In this review, OIG's audit directorate interviewed VA officials and examined email correspondence, call data dashboards, meeting notes, and the relevant and preceding contracts pertaining to these services.

The OIG team maintained continual communication with VCL program office staff and contracting officials throughout this review from December 2025 through May 2026, including the Office of General Counsel; VCL; Office of Information and Technology; and Office of Acquisition, Logistics, and Construction. This report can help contracting officials improve contract oversight and make sure contracted services meet VA information security requirements.

What the Review Found

The OIG found that VA paid about $11.2 million for call responder backup services that were not received. This occurred because (1) VA did not accurately determine the need for an authority to operate to meet federal information security standards until after the new subcontract started and (2) the contracting officer's representative (COR) did not make sure the contractor provided enough backup call responders.

To replace an expiring contract, VA awarded a $32.5 million, firm-fixed-price contract to a contractor to route calls to VCL and provide call responder backup services. The contract included a base year plus four option years and required the backup responder to answer 10 percent of calls and to answer all VCL calls in the event of an emergency. The contractor hired a subcontractor for these services, which represented about $20.5 million (63 percent) of the total contract value. VCL officials and the COR knew as early as about 1.5 months, and the contracting officer knew about 3.5 months, after the new subcontract began that the contractor would not be able to comply with the contract until it met security standards. Nevertheless, VCL officials did not make a decision regarding the contracted services, and the contracting officer did not issue a stop-work order, negotiate a contract modification, or terminate the call responder backup services until almost a year later. According to the Federal Acquisition Regulation

[1] VA OIG, *Veterans Crisis Line Implementation of 988 Press 1 Preparation and Leaders' Response*, Report No. 23-00925-227, August 22, 2024.

1.602-2 and 32.905 (2019), invoices can be approved for services received and the contracting officer is responsible for ensuring contract requirements are met.

The COR accepted the contractor's phased staffing implementation plan that indicated the contractor would have 50 staff about 2.5 months after the new subcontract began and be fully staffed with 92 call responders the following month. However, by the time the call responder backup services were terminated, the backup center had not reached the fully staffed levels specified in the implementation plan.

Since VA officials were aware that services were not received before invoices were approved for payment, the OIG questioned the roughly $11.2 million VA paid for call responder backup services that the contractor did not provide. Under the Contract Disputes Act, codified at 41 U.S.C. §§ 7101–7109, and subject to the applicable statute of limitations, the government has the authority to assert a claim to recoup funds paid for services the contractor did not provide.

The OIG made two recommendations to (1) have the Office of General Counsel determine whether VA should recover the amount paid for undelivered services, and (2) help VA make sure information system security requirements are accurately determined for contracts that involve sensitive information.

Next Steps

The principal executive director of the Office of Acquisition, Logistics, and Construction concurred with recommendation 1 and concurred in principle with recommendation 2 and requested it be closed. The OIG concurred with closing the second recommendation and will close the remaining recommendation upon receipt of sufficient evidence of completed action.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

COR	contracting officer's representative
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
VCL	Veterans Crisis Line
VHA	Veterans Health Administration

Introduction

Suicide prevention is VA's top clinical priority. According to VA's most recent data, the suicide rate among veterans was almost twice that of other US adults, at about 35 suicide deaths per 100,000 veterans.[2] VA established the Veterans Crisis Line (VCL) in 2007, a toll-free, 24/7, confidential resource available to all veterans regardless of whether they are receiving VA benefits or health care. VCL responders—who answer calls and respond to chat and text messages—are trained in crisis management, address the caller's crisis and the caller's level of risk for harm, and initiate dispatch of emergency services if there is a risk of imminent harm. Veterans can reach the crisis line by

- dialing 988 then pressing 1 (implemented by VCL in July 2022),[3]
- texting 838522,
- visiting www.veteranscrisisline.net and clicking the "Chat" button, or
- calling any VA medical center or community-based outpatient clinic and following the instructions.

During a previous review of VCL's implementation of 988 press 1, the VA Office of Inspector General's (OIG) healthcare inspections directorate identified concerns that VA may have paid for VCL call responder backup services it did not receive for over a year and referred its concerns to the VA OIG's audit directorate.[4] Accordingly, the OIG's audit directorate conducted this review to look into these concerns.

In April 2019, VA awarded a $32.5 million firm-fixed-price contract to provide VCL call responder backup services, manage call routing, and manage and maintain the online chat infrastructure to replace an expiring contract.[5] According to the Federal Acquisition Regulation (FAR) 16.202-1 (2019), a firm-fixed-price contract is not subject to any adjustment based on the contractor's cost in performing the contract, and the contractor bears the risk of any lost profits. The contract was for one base year (the initial period of performance) and four option years. The contracting officer could exercise each option year and continue the contract for another year by providing the contractor with a 30-day written notice. The call responder portion of the backup

---

[2] VA Office of Suicide Prevention, *2025 National Veteran Suicide Prevention Annual Report, Part 2: Report Findings*, March 2026.

[3] National Suicide Hotline Designation Act of 2020, Pub. L. No. 116-172, 134 Stat. 832.

[4] The potential contract noncompliance was outside the scope of the OIG's previous report. VA OIG, *Veterans Crisis Line Implementation of 988 Press 1 Preparation and Leaders' Response,* Report No. 23-00925-227, August 22, 2024.

[5] The OIG team's review focused on the call responder backup services portion of the contract. This report refers to "call responder backup services" and the "backup center" interchangeably.

services represented about $20.5 million (63 percent) of the total contract value. The contractor used a subcontract to provide these call responder backup services.

Organizationally, VCL is under the Office of Suicide Prevention within the Veterans Health Administration's (VHA) Clinical Services. VCL business and clinical operations are governed by VHA Directive 1503(2), which lists the responsibilities of the Office of Suicide Prevention, medical facility directors, VCL administrative leaders, VCL staff members, and VHA Suicide Prevention Program staff. In December 2025, VA announced its intent to reorganize the management structure of VHA, and as of June 2026, had completed the initial phase of consolidating contracting specialist under the Office of Acquisition, Logistics, and Construction.[6] The effects of these changes on the issues identified in this report are not yet known.

Contracted Backup Services

The contract's period of performance began on May 1, 2019. In April 2022, the contractor notified the contracting officer's representative (COR) that its original subcontractor planned to terminate the call responder backup center service, which occurred on July 15, 2022. Within about a week of the contractor's notification, VCL leaders partnered with the Office of Information and Technology to create an internal backup system. By May 2022, the internal backup system was minimally operational with additional components to be subsequently added; this internal system was intended to provide basic functionality, ensure the safety of callers, and provide quality care. The contractor engaged a new subcontractor to begin on July 15, 2022, the day before VCL officials adopted the new "988 press 1" hotline number—with no break between subcontracts. See appendix A for a timeline of events.

Contract Requirements

According to the VCL data team supervisory program analyst, VCL call volume is received through two main sources: (1) calls that go directly to the VCL when callers dial local VA medical centers or community-based outpatient clinics and press 7 and (2) calls that flow through the contractor when callers dial 988 and press 1. Calls that flow through the contractor are routed either to the VCL or the backup center.

The contract required backup responders to answer 10 percent of calls that flow through the contractor when callers press 1; this was to maintain proficiency among backup responders, referred to in the contract as "purposeful calls." The calls were to be answered during the contracted operational time, which was initially 12 hours a day, seven days a week; starting September 8, 2022 (during option year 3), operational time was increased to 24 hours a day,

---

[6] VA, "VA launches Veterans Health Administration reorganization," news release, December 15, 2025; VA chief of staff, email to VA OIG, June 18, 2026.

seven days a week. According to the contract, backup responders were also required to handle all calls when the VCL system went down for various reasons such as natural disasters or "any occurrence that adversely impacts the operation or availability of the VCL."

Contract Acquisition Team Responsibilities

The acquisition team for the VCL call responder backup services that determined what security controls were needed before the contract was awarded consisted of the contracting officer and the COR from the Office of Procurement, Acquisition, and Logistics, as well as the information security officer from VA's Office of Information and Technology.

The contracting officer was responsible for ensuring performance of all necessary actions for effective contracting, ensuring compliance with the terms of the contract, and safeguarding the interests of the government in its contractual relationships. To perform these responsibilities, the contracting officer had the authority to enter into, administer, or terminate the contract; to make related determinations and findings; and to delegate some contract management responsibilities to a COR, as set forth in FAR 1.602-1 and 1.602-2 (2019).

The contract specified that the COR was responsible for monitoring contract performance. According to the contract, the COR and the contractor should jointly formulate tactical and long-term courses of action and changes to service levels, procedures, and metrics that would be incorporated as contract modifications by the contracting officer.

The delegation memorandum requires the COR to review the contractor's invoices to verify they accurately reflect the work completed, certify acceptance of the items, and inform the contracting officer as to the satisfactory or unsatisfactory fulfillment of the contract's terms. All invoice payments must be supported by a receiving report or other government documentation that includes a description of services, date of services performed, and the date the designated government official accepted the services, as stated in FAR 32.905 (2019).

The information security officer was responsible for reviewing the proposed performance work statement to ensure the resulting contract sufficiently defined information security responsibilities, provided a means to respond to information security problems, and included a right to terminate the contract if the contractor did not abide by the contract's information security terms. The information security officer was also required to help review, complete, and determine what, if any, security and privacy controls were needed and to advise on the authority to operate process for the contractor's systems, as set forth in VA Handbook 6500.6.[7]

[7] VA Handbook 6500.6, *Contract Security*, March 12, 2010.

Information Security Requirements

VA handles vast amounts of veterans' sensitive healthcare information. This information needs to be accessed from various locations and by many employees. VA is required to follow federal information security standards, including maintaining confidentiality to protect personal privacy; guarding data integrity against unauthorized modification or destruction of information; and ensuring data availability for timely and reliable access to information.[8] Therefore, VA issues an authority to operate after assessing the security and privacy requirements of the information system. In addition, federal and VA policies require that cloud-based applications have Federal Risk and Authorization Management Program (FedRAMP) certification.

Authority to Operate

The process to obtain an authority to operate may require a privacy threshold analysis and a privacy impact assessment to classify a system at the appropriate level. These steps help ensure the system has security controls that match the sensitivity of the information that the system will contain. According to the National Institute of Standards and Technology (NIST), an authority to operate permits staff to use an information system and explicitly accepts the risk to agency operations, assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.[9]

VA considers the need for an authority to operate before awarding contracts for new information systems. VA Handbook 6500.6—related to VA Directive 6500—includes a checklist to determine what, if any, security and privacy controls are necessary.[10] The handbook instructions note that to be successfully completed, each checklist item must be addressed in coordination with all members of the acquisition team: the procurement requestor or program manager (in this case, VCL), the contracting officer, the COR, the privacy officer, and the information security officer. The instructions also note that the "ISO [information security officer] is the arbitrator if there are questions or disagreements on the appropriate answers" to checklist questions.

---

[8] E-Government Act of 2002, Title III—Federal Information Security Management Act of 2002, Pub. L. No. 107-347, §§ 301–305.

[9] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020; NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018.

[10] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021. On April 22, 2024, VA updated the security language in VA Handbook 6500.6, appendix C, "VA Information and Information System Security/Privacy Language for Inclusion into Contracts, as Appropriate" to specify that contracts should be modified if the security requirements change. On March 18, 2025, VA amended Directive 6500 to align with FedRAMP requirements.

FedRAMP

The Office of Management and Budget set the federal policy for protecting federal data in cloud services, which defines executive branch responsibilities for developing, implementing, operating, and maintaining FedRAMP.[11] FedRAMP is a governmentwide program that provides a standardized approach to security, authorization, and continuous monitoring for cloud-based products. It provides a security framework for use across the federal government so agencies can review a standardized set of security materials against one common baseline and enables agencies and cloud service providers to reuse authorizations. Under FedRAMP, a cloud service offering is authorized once, and the related security package can then be used by any federal agency, which potentially saves money, time, and effort for agencies and service providers. VA is required to use FedRAMP when conducting risk assessments, granting security authorizations, and conferring authority to operate for information systems that use cloud services.

[11] Office of Management and Budget, Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011.

Results and Recommendations

Finding: VA Paid for Backup Call Responder Services It Did Not Receive

From mid-July 2022 through June 2023, VA paid about $11.2 million for call responder backup services the contractor did not provide. When the contract was awarded in April 2019, the contracting officer, COR, and information security officer erroneously determined that an authority to operate was not required to safeguard VA sensitive data.[12] VA officials did not re-evaluate the need for an authority to operate until after the new subcontractor started and expressed its plan to use a cloud-based service. Furthermore, the COR approved invoices for payment for services not received and did not ensure the contractor provided enough staff available to answer calls.

The contracting officer told the review team the contractor had to be paid while working toward obtaining the authority to operate, and the contracting officer was waiting for VCL to decide about the backup center. The VCL deputy executive director told the review team that VCL needed a backup system while VA's own internal backup system was developed and implemented. The contracting officer told the OIG healthcare inspections team during its review that the contractor was not taking calls because it was not fully staffed. Subsequently, the contracting officer emailed the team and stated that the contractor had to be paid if they were answering calls. However, VCL and contracting officials were aware that the service was not being provided within 3.5 months of the new subcontract. The COR did not follow the *VA Acquisition Manual* and approved invoices based on the advice of another government employee.[13] The government may assert a claim against the contractor to recoup funds paid for services not received, subject to the statute of limitations under the Contract Disputes Act, as codified in 41 U.S.C. §§ 7101–7109.

What the OIG Did

To evaluate whether call responder backup services were provided, the team reviewed the contract, applicable laws, regulations, and VA policies. The team interviewed VA and VCL officials, reviewed meeting notes and correspondence, and analyzed call data from July 2021 through June 2022 for the number of VCL responders that answered calls. The team also

---

[12] This report discusses two contracting officers and two CORs. The first contracting officer left VA at the end of 2019, and other staff performed contracting officer duties until October 2021 when another contracting officer was assigned. The initial COR transferred to a different VA position, and the subsequent COR appointed in January 2021 is no longer employed at VA. This report uses these position titles to refer to the individual who held the position at the time being discussed.

[13] VA Acquisition Manual, "Contracting Officer's Representative (COR) Guidance," part M801, *Department of Veterans Affairs Acquisition Regulation Systems* (October 2021), M801.604-70.

reviewed call data dashboards and contract invoices from July 2022 through June 2023. Further, the OIG engaged in continuous communication with VCL program office staff and contracting officials throughout the review. In December 2025 and April 2026, the OIG briefed VA leaders, including the Office of General Counsel; VCL; Office of Information and Technology; and Office of Acquisition, Logistics, and Construction. The team also discussed the report findings and recommendations with VA leaders in May 2026. See appendix A for a timeline of significant events and appendix B for more information about the scope and methodology of this review.

Missing Authority to Operate

The information security officer told the OIG team that when completing the information security checklist, the understanding was that VA sensitive data would not be stored in the contractor's system. The official told the OIG team that this determination was based on the performance work statement and discussions with VCL officials. However, the performance work statement required the contractor to transmit call documentation within 30 minutes after a call. Also, the contractor had to record calls and provide the recordings to VCL officials within 24 hours of a request. The contract explicitly stated, "call recordings will be kept according to VA policy; 100% recording and 100% retention."

The OIG team compared the prior 2017 contract to the 2019 contract and noted the requirements for VA sensitive information and call recording were the same. The OIG team also reviewed a sample of backup center call documentation from the original subcontractor and confirmed that some call data included personally identifiable information. The information security checklist in the 2017 contract file indicated an authority to operate was required. According to the information security officer, the understanding was that call recordings would be stored in a VA-owned system that had an authority to operate. The information security officer and the COR who signed the 2019 checklist could not fully explain the discrepancy for the same service requiring an authority to operate for the 2017 contract but not requiring one for the 2019 contract. In March 2023, the COR emailed the contracting officer and stated that the 2019 information security checklist "has been inaccurate since day 1" because "the previous COR documented that the contractor would not store, transmit, or exchange info [information] but the PWS [performance work statement] clearly states that the contractor would." The OIG team noted the handbook does not require a secondary review of the checklist to ensure security needs have been appropriately determined before contract award.

The 2019 COR said, regardless of what was on the information security checklist, the security clauses were included in the awarded contracts to protect VA. The information security officer also explained that this was because changes to requirements may occur. The 2017 and 2019 contracts both included this clause:

> If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after

> execution of the contract, or if NIST issues or updates applicable FIPS [Federal Information Processing Standards] or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

The 2019 contract and information security checklist required an annual contractor security control assessment if sensitive VA information would be stored or transmitted (even if the information system itself did not require an authority to operate). This type of assessment helps define and evaluate information security control mechanisms and practices used by a contractor to safeguard sensitive VA information and offers another opportunity to identify the need for an authority to operate. The OIG team did not find the assessment in the contract file, and the information security officer had neither seen nor completed an assessment and thought it was no longer required. However, VA Handbook 6500.6 requires contractors to conduct an annual security self-assessment on all information systems.

VCL officials did not reevaluate the security controls for the call responder backup services until the subcontractor changed. At the end of August 2022, VCL officials and the COR were included in emails in which the information security officer stated that if the contractor was "processing, storing or transmitting data on behalf of VA then they may be required to have an ATO [authority to operate]." In September 2022, the COR relayed to the contracting officer that the contractor could not use the proposed cloud-based system for document sharing because it needed FedRAMP certification and was not compliant with Federal Information Security Management Act requirements.

In October 2022, the VCL deputy director of technology and innovations sent VCL officials and the COR a draft issue brief that noted it would take 12 to 18 months for the contractor to achieve information system security compliance. By November 2, 2022, the contract had not been modified, and VCL officials, the COR, the contracting officer, and the acquisition services division chief met to discuss the authority to operate and FedRAMP requirement. According to the meeting notes, the contractor could not provide backup responder services without an authority to operate. These meeting notes demonstrate that by early November 2022, the contracting officer was aware that the contractor could not provide the contracted call responder backup services due to the lack of authority to operate.

Contractor Staffing Issues

The COR's oversight of the contract also did not ensure the contractor provided sufficient backup call responders to answer the required 10 percent of calls. The contractor was required to provide enough staff to answer all calls in the event of an emergency where VCL could not answer any calls. According to VCL records, about 600 VCL responders on average answered calls each month during the 12 months preceding July 2022. The VCL division director of quality assurance and risk management told the OIG team that during the review period, the contractor would need to provide 60 employees for adequate backup coverage for the projected call volume. The team noted that 60 would represent 10 percent of VCL responders, and the contract required the backup center to answer 10 percent of VCL's calls that flow through the contractor when callers press 1, as well as all calls if necessary.

The contractor provided the COR with a phased implementation plan for the new subcontractor who was scheduled to begin the same day the previous subcontract ended. The COR evaluated and rated the implementation plan as acceptable in July 2022 during a technical evaluation for a proposed contract modification to increase the call responder backup services from 12 hours a day to 24 hours a day, effective September 2022. The plan stated that 50 staff would be on board by October 2022, about 2.5 months after the new subcontract began, and the backup center would be fully staffed at 92 call responders by the following month. However, according to the contractors' hiring schedule, the contractor did not reach 50 staff until eight months after the planned date and did not achieve full staffing levels before the call responder backup services were terminated in June 2023. According to the VCL division director of quality assurance and risk management, the new subcontractor was a crisis center; therefore, its staff could answer 988 calls in cases where veterans chose not to press 1.

Services Not Delivered

During the previously discussed November 2, 2022, meeting, the VCL deputy executive director noted that the contractor was hiring staff but was at least one to two years away from providing services. Additionally, the meeting notes included a section regarding paying for services not received, and the COR told the OIG team that VCL leaders had expressed concerns to the contracting officer about that issue. The meeting minutes note that the acquisition services division chief suggested the contracting officer could modify the contract, which would require negotiations on price-related factors, or issue a stop-work order for 60 days to allow time to decide how to move forward with the call responder backup services. The contracting officer told the meeting attendees that the contractor must be given a chance to become compliant and had to be paid. During the prior OIG healthcare inspection directorate's review, the contracting officer told the team the contractor should be paid during the implementation but "not if they were invoicing for taking calls if they were not taking calls." However, the contracting officer had previously told the healthcare inspection directorate's team the contractor was not taking calls because it was not fully staffed. The OIG determined that the contractor continued to be paid for call responder backup services not provided, indicating inadequate contract oversight.

The OIG review team asked the contracting officer why action suggested in the November 2, 2022, meeting had not occurred. The contracting officer told the team that the contractor should be given the opportunity to comply with the security requirements, and he had waited for VCL officials' direction. The team pointed out the contracting officer's responsibilities to ensure contract compliance, safeguard the government's interests, terminate contracts, and make related determinations and findings, as well as the requirement to pay only for services received (FAR 1.602-1, 1.602-2 and 32.905 (2019)). However, the contracting officer repeated that a decision would not be made without VCL officials' instruction. As noted, the VCL deputy executive director told the OIG team that, while VCL's own internal backup system was being developed and implemented, a backup system was needed.

VCL officials, the COR, the contracting officer, and the information security officer met November 10, 2022. According to the meeting notes, the contractor would not be able to receive calls for at least nine to 18 months while pursuing security certifications and exploring alternative solutions. The contracting officer did not recommend a stop-work order option but did recommend a modification to the contract language for security compliance.

The OIG team asked the acquisition services division chief about paying for services not received. Despite having heard at the November 2, 2022, meeting that it would be at least one to two years before services would be provided, the chief told the OIG team there was no evidence in the contract file that indicated the contractor did not provide call answering services. The chief also noted that VCL officials did not provide a formal written notification stating that services were not being provided. Although not a requirement, the chief told the OIG team that the contracting officers are instructed not to take contract action without written directions from a VA official with the authority to do so.

The contracting officer emailed the OIG healthcare inspections team during its prior review and said, "at one point, someone from VCL told [the contractor], without any official CO [contracting officer] authorization, to not take calls and I don't know who, why or when." The day after that email, the contracting officer sent the contractor a memorandum stating that any direction regarding the contract shall and must be directly from the authorized contracting officer and no one else (unless the COR had been designated the authority from the contracting officer).

The OIG team analyzed the calls routed to the backup center from July 2022 through June 2023. Based on the data, four calls were directed to the backup center on July 9, 2022, before the new subcontractor started. Two calls were sent to the backup center in August 2022; according to the VCL data and workforce management division director, the two August calls were probably not answered based on the length of each call. The data shows, with the exception of the two calls in August, that the contractor did not transfer calls to the call responder backup center from mid-July 2022 through June 2023.

Nevertheless, on March 1, 2023, a VCL management analyst emailed the VCL executive director stating VCL would like to exercise the next contract option year for the backup center. The email also indicated that the internal backup system was not fully developed and implemented. That same day, the VCL executive director approved exercising the next contract option year. The next day, the COR issued an exercise option year memorandum to the contracting officer with an evaluation that indicated satisfactory contractor performance. However, as noted, VCL and contracting officials were aware in November 2022 that services could not be performed without an authority to operate and, based on the data, the contractor did not provide the contracted call responder services. The contracting officer issued the modification to continue the contract on April 5, 2023, meeting the 30-day notice requirement to exercise an option. As of the end of that month, VA had paid about $9.2 million for call responder backup services that were not received.

As noted, an invoice payment must be supported by the date the government official (in this case, the COR) accepted the services rendered. The COR told the OIG team that invoices were approved for payment based on the contracting officer's advice that payments were justified under the type of contract (firm-fixed-price) and because the contractor was making progress during the implementation phase and working toward an approval for an authority to operate. Thus, the COR approved monthly invoices for payments for call responder backup services that were not provided. However, the *VA Acquisition Manual* M801.604-70 (2021) states, "the COR should not recommend invoice payment solely on the recommendation of another government employee."[14]

In May 2023—the first month the new option year began—the VCL deputy executive director notified the COR of the decision to terminate the call responder backup services portion of the contract. The COR relayed the decision to the contracting officer. The contracting officer issued the termination memorandum on June 28, 2023. VA and the contractor agreed VA would pay $677,575 in settlement costs for the partial contract termination of the call responder backup services part of the contract. According to FAR 52.212-4 (2019), contractors shall be paid a percentage of the contract price based on the work performed before the notice of termination.

VCL and contracting officials' could have acted sooner to negotiate a contract modification, issue a 60-day stop-work order, or terminate the call responder backup services. Instead, the delay in action contributed to VA paying about $11.2 million for almost one year of call responder backup services that were not provided and $677,575 in settlement costs. Including these settlement costs, VA paid about $11.9 million for services that were not received; however, the OIG team excluded settlement costs from the questioned amounts. Questioned costs are reported by the OIG in accordance with the Inspector General Act of 1978, as amended.[15] For more information on questioned costs, see appendix C.

Conclusion

VA's oversight of this contract fell short. While the contract contained security clauses to protect VA sensitive data, VA did not verify the accuracy of the information security checklist during contract acquisition. A careful review of the information security checklist may have identified

[14] VA Acquisition Manual, "Contracting Officer's Representative (COR) Guidance," part M801, *Department of Veterans Affairs Acquisition Regulation Systems* (October 2021), M801.604-70.

[15] 5 U.S.C. § 405.

the need for an authority to operate before the contract was awarded. The contracting officer and COR also did not make sure the contractor completed a security self-assessment in accordance with VA Handbook 6500.6, which was a missed opportunity to identify the need for an authority to operate. In addition, the COR did not ensure the contractor provided enough staff for the call responder backup services as outlined in the approved implementation plan.

VA should confer with the Office of General Counsel to determine whether the $11.2 million VA paid for services not received should be recouped under the Contract Disputes Act, codified at 41 U.S.C. §§ 7101–7109. VA should also consider what steps should be taken to verify the acquisition team accurately determines information system requirements for contracted services. While the effects of VA's reorganization on the issues identified in this report are not yet known, the findings can help inform VA's oversight of contracts and information security going forward.

Recommendations 1–2

The OIG made the following recommendation to the principal executive director and chief acquisition officer of VA's Office of Acquisition, Logistics, and Construction:[16]

1. Confer with the VA Office of General Counsel to determine whether VA should assert a claim to recover the $11.2 million paid for services not received.

The OIG made the following recommendation to the principal executive director and chief acquisition officer of VA's Office of Acquisition, Logistics, and Construction and to the principal deputy assistant secretary of Office of Information and Technology:

2. Evaluate and take any needed actions to make sure policies and procedures require appropriate officials to accurately ascertain information security requirements for contracts that involve sensitive information prior to award.[17]

VA Management Comments

The principal executive director, who also serves as the chief acquisition officer, of the Office of Acquisition, Logistics, and Construction concurred with the first recommendation and will confer with the VA Office of General Counsel. He concurred in principle with the second recommendation and acknowledged the error that resulted in incorrectly determining that the information system did not require an authority to operate. According to the principal executive director, VA addressed the issue with the acquisition team and reinforced applicable requirements to reduce the likelihood of this error happening again. He further noted that this

[16] The recommendations are addressed to the principal executive director and chief acquisition officer of the Office of Acquisition, Logistics, and Construction because of VA's reorganization that is in process. The recommendations are directed to anyone in an acting status or performing the delegable duties of the position.

[17] After discussing the report findings and recommendations with VA leaders on May 7, 2026, the OIG revised the second recommendation.

issue did not reflect a systemic breakdown in acquisition or security governance processes and requested closure of the recommendation. The full text of VA's management comments is presented in appendix D.

OIG Response

The corrective action plans provided by the principal executive director and chief acquisition officer at the Office of Acquisition, Logistics, and Construction are responsive to the intent of both recommendations. The OIG concurs with closing the second recommendation and will close the remaining recommendation once sufficient evidence has been provided.

Appendix A: Timeline of Events

Some events related to the contracted call responder backup services for the Veterans Crisis Line (VCL) are displayed in figure A.1.

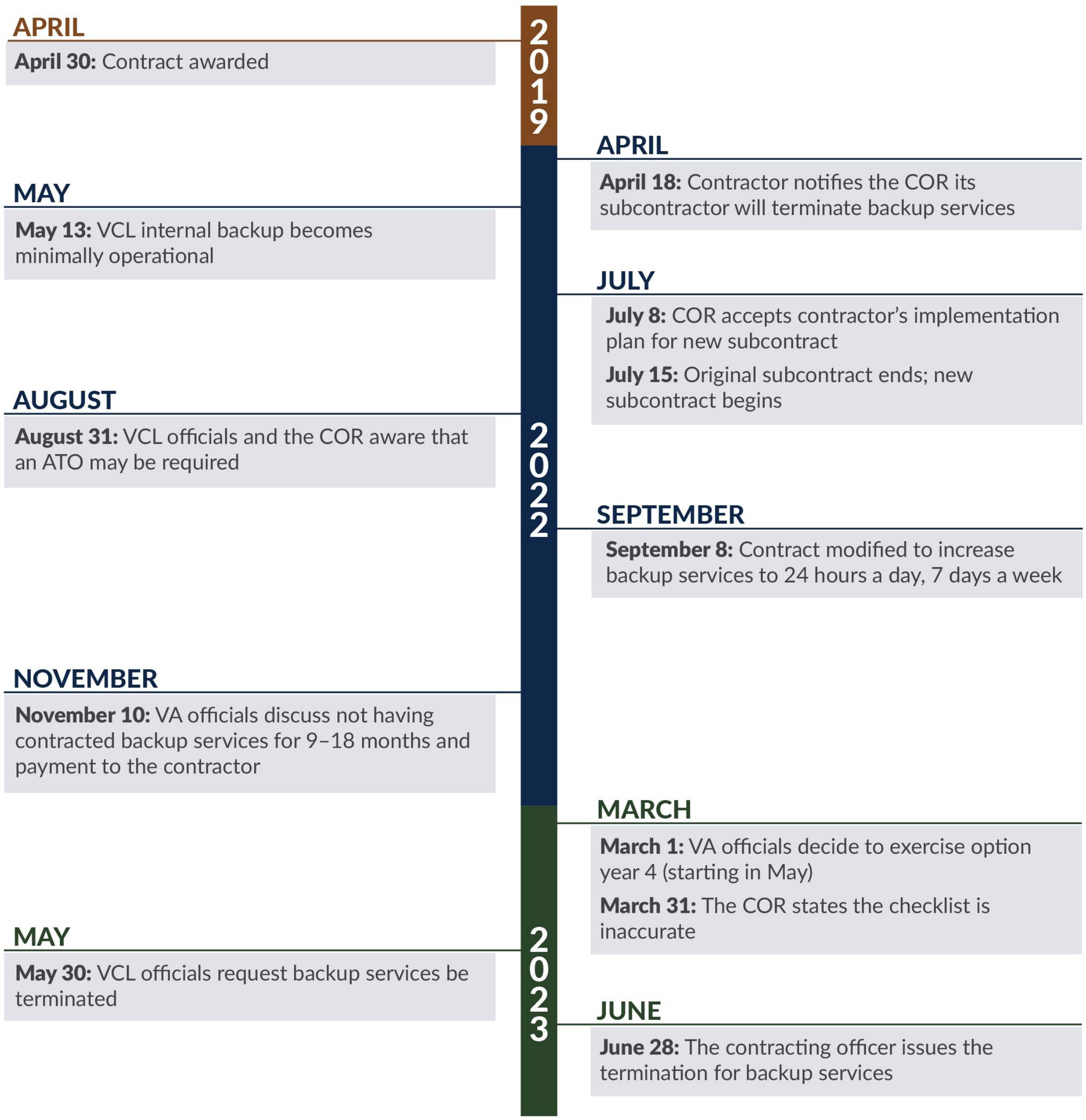

Figure A.1. *Timeline of events related to the contracted call responder backup services for the Veterans Crisis Line.*

Note: COR stands for contracting officer's representative. VCL stands for Veterans Crisis Line. ATO stands for authority to operate.

Source: VA OIG analysis of contract information and VCL documentation.

Appendix B: Scope and Methodology

Scope

The VA Office of Inspector General (OIG) audit directorate team conducted its work from November 2024 through April 2026. The team assessed a universe of 13 invoices for Veterans Crisis Line (VCL) call responder backup services totaling about $11.5 million, dated from July 2022 through June 2023; contract documentation; and VA websites. The team also interviewed VA officials.

Methodology

The team identified and analyzed applicable laws, regulations, VA information system policies and procedures, VA acquisition policies and procedures, and relevant records. To verify call responder backup service payments made to the contractor, the team used VA's Invoice Payment Processing System. The team also interviewed VCL leaders and staff, the information security officer, and Office of Procurement, Acquisition, and Logistics contracting officials. In addition, the team reviewed email correspondence, call data dashboards from July 2022 through June 2023, meeting notes pertaining to the call responder backup services, information obtained during the OIG's healthcare inspections review, and documentation obtained from VA's Electronic Contract Management System for the VCL 2017 and 2019 contracts.

Internal Controls

The team assessed internal controls to determine whether they were significant to the review objective. This included consideration of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring. In addition, the team reviewed the principles of internal controls associated with the objective and identified two components and two principles as significant. The team identified internal control deficiencies during this review and proposed recommendations to address those listed in table B.1.

Table B.1. VA OIG Analysis of Internal Control Components and Principles Identified as Significant

Component	Principle	Deficiency identified by this review
Control environment	5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.	VA officials did not take timely action to prevent paying for services not received.

Component	Principle	Deficiency identified by this review
Monitoring	17. Management should remediate identified internal controls deficiencies on a timely basis.	VA officials did not take timely action to modify the contract or terminate the call responder backup services.

Source: VA OIG analysis of internal control components and principles consistent with the Government Accountability Office's Standards for Internal Control in the Federal Government.

Data Reliability

Computer-processed data used for this review were determined to be reliable for the purpose of this review. The OIG team obtained invoices from the VA Invoice Payment Processing System and assessed the reliability of these data by comparing contract line item number prices to the invoices. The team discussed the contractor's implementation plan and hiring schedule with VCL officials. Contract documentation obtained from VA's Electronic Contract Management System was also discussed with contracting officials. The OIG believes the data and documents obtained are sufficiently reliable to support its objectives, conclusions, and recommendations.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.[18]

[18] Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*, December 2020.

Appendix C: Monetary Benefits in Accordance with Inspector General Act Amendments

Recommendation	Explanation of Benefits	Better Use of Funds	Questioned Costs[19]
1	Payment for Veteran Crisis Line backup responder services not received.	$0	$11,200,000
	Total	**$0**	**$11,200,000**

[19] The OIG questions costs when VA action or inaction (such as spending or failure to fully compensate eligible beneficiaries) is determined by the OIG to violate a provision of law, regulation, contract, grant, cooperative agreement, or other agreement; when costs are not supported by adequate documentation; or when they are expended for purposes that are unnecessary or unreasonable under governing authorities. Within questioned costs, the OIG must, as required by section 405 of the IG Act, report unsupported costs. Unsupported costs are those determined by the OIG to lack adequate documentation at the time of the audit. Of the $11,200,000 in questioned costs, $0 were unsupported costs. The OIG team did not include costs for the first half of July 2022 nor the settlement costs in the questioned costs.

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: July 30, 2026

From: Principal Executive Director, Office of Acquisition, Logistics, and Construction (003) and Chief Acquisition Officer

Subj: Office of Inspector General (OIG) Draft Report: Review of Contracted Backup Services for the Veterans Crisis Line (2023-03464-AE-0137) (VIEWS 14686956)

To: Office of Inspector General (50)

The Office of Acquisition, Logistics, and Construction has completed its review of the subject Office of Inspector General draft report and provides the attached comments.

The OIG removed point of contact information prior to publication.

(Original signed by)

Phillip W. Christy

Attachment

Attachment

Department of Veterans Affairs (VA) Draft Report Comments
Office of Inspector General (OIG)
Review of Contracted Backup
Services for Veterans Crisis Line (VCL)
(2023-03464-*AE-0137)*
July 2026

Recommendation 1: Confer with the VA Office of General Counsel to determine whether VA should assert a claim to recover the $11.2 million paid for services not received.

VA Response: Concur. The Office of Acquisition, Logistics, and Construction (OALC) will confer with the Office of General Counsel to determine if VA should assert a claim to recoup those funds.

Status: In Progress **Target Completion Date:** December 31, 2026

Recommendation 2 (revised):[20] Evaluate and take any needed actions to ensure policies and procedures require appropriate officials to accurately ascertain information security requirements for contracts that involve sensitive information prior to award.

VA Response: Concur in Principle. VA has established policies and procedures to ensure security requirements for contracts involving sensitive information are identified and documented prior to award. VA Directive 6500, VA Handbook 6500.6, and the VA Acquisition Regulation collectively provide the framework for integrating information security and privacy requirements into the acquisition process. These requirements define the roles and responsibilities of acquisition stakeholders, including the Contracting Officer (CO); Contracting Officer Representative (COR); Program Office; Privacy Officer; Information Security Officer (ISO); and the Information System Security Officer. The requirements establish the process for determining and applying appropriate security and privacy controls when VA sensitive information is involved.

In this case, the acquisition team generally followed established policies and procedures throughout the procurement process; however, an error occurred during completion of VA Handbook 6500.6 checklist, resulting in the determination that an Authority to Operate (ATO) was not required for this effort.

VA addressed the issue with the acquisition team and reinforced applicable requirements to reduce the likelihood of recurrence. Based on the review conducted, VA does not believe this issue reflects a systemic breakdown in enterprise acquisition or security governance processes. VA requests closure of this recommendation based on the evidence provided in the attachments.

Supporting Documentation: VA Directive 6500, VA Handbook 6500.6, VA Notice 24-12, VA Notice 24-18, and VA Notice 25-07.

The text of VA's management comments is reprinted verbatim as received from the department. For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

[20] The OIG revised recommendation 2 following a collaborative call with Office of Information Technology and OALC staff in May 2026.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Review Team	Alyssa Witten, Director Valerie Kimball Nancy Soto
Other Contributors	Khaliah McLaurin Jill Russell

Report Distribution

VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Procurement, Acquisition, and Logistics
Office of Public and Intergovernmental Affairs
Veterans Health Administration

Non-VA Distribution

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

Pursuant to Pub. L. No. 117-263 § 5274, codified at 5 U.S.C. § 405(g)(6), nongovernmental organizations, and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference to the organization or entity. Comments received consistent with the statute will be posted on the summary page for this report on the VA OIG website.

OIG reports are available at vaoig.gov.