

## Independent Assessment and VA Response Generally Met Requirements

GAO-26-107980

December 2025

A report to congressional committees.

For more information, contact: Jennifer Franks at [franksj@gao.gov](mailto:franksj@gao.gov).

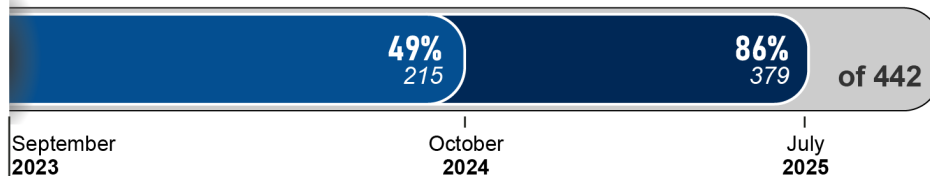
## What GAO Found

Based on a requirement in the Strengthening VA Cybersecurity Act of 2022, the Department of Veterans Affairs (VA) contracted with MITRE to perform a cybersecurity assessment. The subsequent assessment addressed the requirements in the act and aligned with federal guidance. For example, MITRE appropriately (1) selected for review five key systems that, if compromised, could severely impair VA's ability to execute its mission, and (2) evaluated the effectiveness of VA's information security program.

VA submitted a plan to remediate the findings identified by the assessment that generally addressed the requirements in the act. Specifically, the remediation plan included a cost estimate and implementation timelines to address the system and security program findings. The remediation plan also included planned improvements to VA's security program. While the remediation plan did not include improvements to system-specific security controls, VA provided details on those plans in other documents.

VA has reported progress in remediating findings across the five systems and its security program. Specifically, the department reported remediating 215 of 442 system-specific findings by October 2024 and remediating 379 findings by July 2025 (see figure). Also, the department reported that it had completed 20 of 55 actions to address the 11 information security program findings.

### VA reported remediation progress on 442 system findings



• MITRE began to report findings to Department of Veterans Affairs (VA)

Source: GAO analysis of VA reported remediation progress. | GAO-26-107980

VA generally documented remediation efforts for the system and program findings in accordance with federal requirements. However, it did not always update its remediation plans. For example, for one system, VA did not update the remediation date for a high-risk vulnerability that was 15 months past due. Similarly, the department did not update estimated remediation dates for at least two program findings. Further, although plans were in place, remediation efforts were not timely. Specifically, as of July 2025, VA had not remediated two high-risk vulnerabilities—those with the most severe consequences—over a 17 to 21-month period, although its policy is to remediate them within 60 days.

VA's Inspector General has previously made recommendations to VA to (1) ensure the department tracks and updates planned remediation documents and (2) improve the process for resolving vulnerabilities that cannot be addressed within policy timeframes by ensuring implementation of mitigating controls. As of July 2025, VA had not yet implemented these recommendations. Doing so would help ensure that needed actions are taken to protect systems.

## Why GAO Did This Study

VA depends on critical IT systems to manage benefits and provide health care to veterans and their families. VA's highly networked and technologically diverse systems create unique cybersecurity complexities. Protecting these systems from cyber threats is imperative.

The Strengthening VA Cybersecurity Act of 2022 includes a provision for GAO to evaluate an independent cybersecurity assessment and VA's remediation plan in response to the assessment. This report examines the extent to which (1) the independent cybersecurity assessment addressed the act and federal guidance, (2) VA's remediation plan adhered to the act, (3) the department reported remediating the assessment's findings, and (4) VA's efforts to remediate selected findings adhered to federal requirements.

To address these objectives, GAO compared MITRE's assessment of selected systems and the overall information security program, as well as VA's remediation plan, against requirements in the act. GAO also summarized VA's reported remediation progress for the assessment findings. In addition, GAO compared VA's efforts to remediate findings against federal requirements. Further, GAO interviewed relevant MITRE and VA officials.