INSPECTOR GENERAL'S FRAUD WATCH

JULY 2026

The VA OIG fights fraud through close collaboration with VA personnel, federal law enforcement partners, the Department of Justice, and multiple fraud task forces, including the Fraud Task Force established by the President's March 2026 Executive Order. VA OIG staff investigate and deter fraudulent and criminal conduct and disrupt complex fraud schemes that impact veterans' healthcare, education, and benefits.

Recent enforcement actions and audit reports included below highlight this impact. You can find more information on the VA OIG's oversight work, along with full investigative updates and reports, by visiting the VA OIG website.

Investigations – Recent Activity and Ongoing Cases

Healthcare Fraud

Healthcare fraud by VA-paid healthcare providers and vendors in the community is the intentional misrepresentation of information to gain payment, inconsistent with the type, scope, or nature of the treatment, service, or product provided.

- An Orlando VA employee and the Chief Executive Officer (CEO) of a VA Community Care Program medical group pleaded guilty to conspiracy to pay and receive health care kickbacks. A VA OIG and FBI investigation resulted in charges alleging that Heriberto Rivera, the CEO of Family Integrative Medicine of Orlando, LLC ("FIMO"), paid kickbacks to Laurent Cassagnol, a VAMC Orlando employee, in exchange for Cassagnol sending VA patients to FIMO. FIMO then billed VA for services it provided to those VA patients. Rivera paid Cassagnol approximately $175,172 in kickbacks, which resulted in approximately $14,080,969 in claims submitted by FIMO to VA that were procured through the payment of kickbacks. VA paid FIMO approximately $11,948,349 on those claims.

- A Maryland oncology practice and its owner agreed to pay over $1.4 million to settle fraudulent billing allegations under the False Claims Act. A VA OIG and Department of

Health and Human Services OIG investigation resulted in a settlement that resolved allegations that Progressive Oncology and Hematology, LLC (Progressive) and its owner, Dr. Mouhamad Bazzi, knowingly submitted claims to VA, Medicare, and Medicaid to reimburse the practice for chemotherapy drugs that the defendants never actually purchased. The settlement resolved allegations that Progressive and Bazzi submitted claims for reimbursement for drugs paid for and supplied by charitable organizations or through grant programs for specific patients at no expense to the defendants. Additionally, the defendants allegedly directed that wastage (small amounts of extra medication) from single-use vials of drugs intended for one patient be split across two or more patients. The defendants allegedly then submitted claims as if each patient received their own single-use vial. Further, Progressive and Bazzi allegedly billed federal and state health insurance programs for chemotherapy drugs Bazzi prescribed but never actually administered.

- A nonveteran was sentenced to 21 months' home confinement, 24 months' supervised release, and restitution of about $11,500,000 for his role in durable medical equipment fraud. The estimated VA loss was $330,000.

- A VA OIG investigation resulted in charges alleging health care fraud, aggravated identity theft, and false statements. The defendant allegedly received approximately $30,000 in VA medical care and services by assuming the identity of a veteran. The defendant also allegedly received housing through a non-profit organization that provides housing and support services to veterans through VA's Supportive Services for Veteran Families program. The charges further alleged the defendant received $374,000 in other fraudulent services and benefits from the Social Security Administration, Medicaid, and the New York City Human Resources Administration. As a result of a prior VA OIG investigation, the defendant was previously sentenced to 36 months' imprisonment for committing aggravated identity theft against the same veteran.

- A nonveteran who is a registered sexual offender was sentenced to 48 months' incarceration and 36 months' probation and was ordered to pay VA $28,118 in restitution for theft of government funds. A VA OIG investigation revealed that, although VA databases listed the defendant as an Army veteran, there were no corresponding records that the defendant ever served in the military. A review of VA healthcare records confirmed that VA paid $83,369 for treating the defendant from 2022 to 2023. The defendant also allegedly submitted a forged DD-214 military discharge document to the

State of Florida's Support Services for Veteran Families to temporarily obtain veteran housing. Due to the VA OIG investigation, the defendant provided substantial assistance to the government for an unrelated child exploitation, enticement, and child pornography investigation that helped convict another defendant.

- The owner of a home healthcare company was sentenced to 18 months' imprisonment and 36 months' supervised release and was ordered to pay restitution in the amount of $210,315 after previously pleading guilty to wire fraud. A VA OIG and Missouri Medicaid Fraud Control Unit investigation revealed that, from August 2020 to December 2022, the defendant submitted fraudulent claims to VA and Missouri Medicaid for services that were never provided. The defendant submitted fraudulent claims for services reportedly performed while veterans were inpatients at VA Medical Centers and for patients who allegedly received more than 24 hours of care in a single day. As part of the defendant's plea agreement, she admitted to a total fraud loss of $210,315; the loss to VA was approximately $100,563.

- The owner of a home health company self-surrendered after previously being charged with healthcare fraud. A VA OIG and FBI investigation resulted in charges alleging that the defendant and his company submitted false claims for payment to VA's third-party administrator for home health services that were not provided. It is further alleged that the defendant and his company submitted false claims for a greater number of care hours than those provided to infirm veterans. The defendant allegedly used the fraudulently obtained VA funds to pay for sports gambling and other personal expenses. The loss to VA was approximately $371,981.

- A nonveteran was charged with forgery, theft, and attempt to influence a public servant. The defendant allegedly submitted a fraudulent DD-214 to obtain VA healthcare services and treatment valued at $16,783, despite never serving in the military. The defendant also allegedly submitted additional counterfeit DD-214s, bogus VA treatment records, and photos of his late father's military awards that he attempted to pass off as his own throughout nine unsuccessful attempts to obtain VA disability compensation benefits. The loss to VA was $16,783.

- A medical device company entered into a settlement agreement to resolve allegations that the company's sales team fabricated medical records to submit claims for payment and justify the costs to VA for an unnecessarily expensive pneumatic compression device.

The company agreed to pay a total of $550,959, with $275,479 earmarked for Medicare. VA spent a total of approximately $1.5 million on the devices, but a statistical claims analysis did not identify any VA damages. The investigation was conducted by the VA OIG, the Department of Health and Human Services OIG, FBI, Defense Criminal Investigative Service, the United States Postal Service OIG, and the Office of Personnel Management OIG.

- A chiropractor and owner of a medical supply company was convicted of conspiracy to commit healthcare and wire fraud. An investigation by the VA OIG, the Department of Health and Human Services OIG, Defense Criminal Investigative Service, and FBI resulted in charges alleging the defendant paid illegal kickbacks to marketers in exchange for referral of Medicare patients, and to marketers and telemedicine companies in exchange for signed doctors' orders that could be used to support claims to government healthcare programs even though the telemedicine providers did not engage in meaningful patient evaluations before signing the orders. This scheme resulted in approximately $30 million in false and fraudulent claims to multiple government healthcare programs, including approximately $92,440 to CHAMPVA, for durable medical equipment that was medically unnecessary, obtained through the payment of illegal kickbacks, and not provided as billed.

- A diagnostic laboratory sales representative was charged for allegedly conspiring to solicit providers to issue orders for unnecessary respiratory panel tests to be bundled with COVID-19 tests to maximize reimbursement from healthcare benefit programs. The defendant and others allegedly capitalized on COVID-19 testing shortages by offering providers short turnarounds on COVID-19 tests but only if they were ordered in combination with medically unnecessary—and far more expensive—respiratory panel tests. To conceal the fraud, they allegedly instructed providers to add false diagnostic codes when testing asymptomatic patients and concealed the billing codes from the medical providers to hide the bundling of the expensive and medically unnecessary respiratory panel testing when they knew providers intended to order only a COVID-19 test. The defendant allegedly caused the submission of over $51.7 million in claims to healthcare benefit programs, of which the programs reimbursed over $28.4 million. The total estimated billed amount to all healthcare benefits programs was $120 million, of which approximately $60 million was paid. The loss to VA loss was approximately $200,000. This investigation was conducted by the VA OIG, the Louisiana Medicare

Fraud Control Unit, Defense Criminal Investigative Service, the Department of Labor OIG, the Department of Health and Human Services OIG, and the FBI.

- The owner of a marketing company was sentenced to 24 months of supervised release, during which 21 months will be served in home detention, and was ordered to pay restitution of approximately $11.5 million for his role in a conspiracy to defraud the government in connection with a scheme to violate anti-kickback and health care fraud statutes. The defendant and others allegedly participated in a healthcare fraud scheme where telemarketers solicited DME and CGXs to prospective patients. Telemedicine doctors, with whom the patients did not have an existing relationship, wrote the resulting prescription orders. Many of the companies identified in the scheme billed CHAMPVA. The total loss to VA was approximately $330,000. To date, investigative efforts have led to 24 arrests and 22 convictions. This investigation was conducted by the VA OIG, the FBI, the Department of Health and Human Services OIG, and Defense Criminal Investigative Service.

Fiduciary Fraud

VA's Fiduciary Program was established to protect veterans and other beneficiaries who are unable to manage their financial affairs due to injury, disease, or age-related issues. Fiduciary fraud involves the theft of benefits by a VA-appointed fiduciary who is supposed to manage VA beneficiaries' finances in their best interests.

- A former VA-appointed fiduciary was sentenced to 24 months' imprisonment and 24 months' supervised release and was ordered to pay $133,133 in restitution after previously pleading guilty to misappropriation by a fiduciary. A VA OIG investigation revealed that between November 2015 and November 2022 the defendant comingled the funds of multiple VA beneficiaries with her personal accounts. The defendant spent the veterans' money on shopping, restaurants, travel, bill payments, and other personal expenditures. The investigation also determined the defendant was in a personal relationship with the VA field examiner who oversaw her activities. The field examiner was terminated by VA in December 2024 as a result of this investigation.

- The niece of a veteran who previously served as his VA-appointed fiduciary pleaded guilty to theft of government funds. A VA OIG and Social Security Administration OIG investigation resulted in charges alleging that between October 2021 and March 2024 the defendant withdrew $114,660 in VA benefits and $45,734 in Social Security benefits

from the veteran's bank accounts without permission and for her own personal use, which included gambling expenses.

- The daughter of a veteran who previously served as his VA-appointed fiduciary was sentenced to 60 months' probation and ordered to pay restitution in the amount of $49,060. A VA OIG investigation revealed that the defendant spent VA benefits totaling $49,060 that were intended for the veteran. During an interview with VA OIG agents, the defendant admitted that she used the veteran's funds for her own personal use. The defendant is also a Topeka, Kansas, VA medical center customer service representative who has been placed on indefinite suspension pending judicial actions.

Pension and Dependency and Indemnity Benefits Fraud

VA pension benefits are available to wartime veterans or their survivors who meet certain age or disability requirements and have limited income and net worth. VA pension beneficiaries who need help with daily activities or are housebound may be eligible for an additional monetary payment. Veterans are targets of wide-ranging "pension poaching" schemes that attempt to steal their assets. Dependency and Indemnity Compensation (or DIC) benefits are for the surviving spouse, child, or parent of a service member who died in the line of duty, or the survivor of a veteran who dies from a service-related injury or illness.

- The son of a deceased VA beneficiary was sentenced to 60 months' probation and ordered to pay $134,720 restitution to VA. A VA OIG investigation revealed the defendant continued to collect and withdraw his deceased mother's VA Dependency and Indemnity Compensation benefits following her death in December 2018. During an interview with VA OIG agents, the defendant admitted that he withdrew cash from his mother's bank account following her death and used the money for personal gain. The loss to VA was approximately $134,720.

Computer Fraud

Computer crime, also known as cybercrime, refers to illegal activities committed using computers or digital networks to steal, damage, or manipulate information for personal, financial, or political gain.

- A veteran and co-conspirator were convicted for their scheme to target seriously ill veterans for fraud. A VA OIG investigation into identity theft found that, from December

2021 to September 2022, an Army veteran, while incarcerated, made approximately 2,435 telephone calls to 11 different VA facilities. During these calls, the subject requested and received numerous call-transfers to at least 26 VA medical centers, where he successfully used various ruses and social engineering techniques to fraudulently obtain 369 US Veteran patient names, Veteran emergency contacts data, and personally-identifiable information (PII). With the assistance of a co-conspirator, subsequent calls to veterans and veteran emergency contacts resulted in obtaining 63 financial accounts and additional PII. The investigation identified more than 60 victims and 130 fraudulent transactions, which resulted in an approximate loss of $8,000.

VA Loan Guaranty Fraud

VA provides home loan guaranty benefits and other housing-related programs to help veterans, servicemembers, and eligible surviving spouses become homeowners.

- A veteran who was a Department of Homeland Security employee was arrested after being criminally charged with wire fraud and false statements related to a mortgage. A VA OIG investigation resulted in charges alleging that the defendant submitted false documents to obtain a VA-backed mortgage. The documents allegedly embellished the defendant's VA disability rating and monthly VA disability benefits payments and falsely claimed he was exempt from paying a VA funding fee. As a result of the defendant's alleged misrepresentations, he received a VA-backed mortgage loan of $478,000.

Compensation Benefits Fraud

Compensation benefits fraud involves individuals' submission of fraudulent claims for payment of VA disability benefits.

- A veteran employed as a Military Service Coordinator was indicted on five counts of mail fraud and two counts of false claims. A VA OIG and US Postal Inspection Service investigation resulted in charges alleging that between January 2020 and May 2025 the defendant prepared at least 925 fraudulent VA disability claims. The indictment also alleged that the employee concealed her VA employment and portrayed her business and actions as legitimate to receive payments from veterans who were applying for VA disability compensation. As alleged, despite lacking VA accreditation to assist veterans with their claims, and while employed by VA, the defendant advertised services to veterans, guaranteed 100 percent disability ratings, and coached claimants to assert fabricated medical conditions using prewritten templates. The defendant allegedly

collected between $1,000 and $3,500 per veteran for her services and received at least $925,000 in electronic transfers and cash from the fraud scheme. A search of the defendant's residence recovered close to $120,000 in cash.

- A former VA employee was indicted on charges of wire fraud and attempting to commit wire fraud. A VA OIG, Coast Guard Investigative Service, and General Services Administration OIG investigation revealed that the defendant allegedly submitted a fraudulent Certificate of Release or Discharge from Active-Duty Form 214 (DD-214) to VA when applying for VA benefits, to include disability compensation, education, pre-burial, and healthcare. The defendant allegedly claimed he had a period of service in the Coast Guard with an honorable discharge. However, during an interview with VA OIG agents, the defendant allegedly admitted that he never served in the military.

- Two nonveteran suspects were indicted on charges of conspiracy to receive stolen treasury checks, receipt of stolen government property, and aggravated identity theft. A joint VA OIG investigation with the Treasury Inspector General for Tax Administration resulted in charges alleging that the defendants operated a multi-state scheme involving opening fraudulent bank accounts under aliases and depositing stolen US Treasury checks, including VA benefits checks and IRS tax refunds. A search warrant resulted in the recovery of fake identification documents along with stolen Treasury checks, including checks issued by VA intended for veterans living in Florida, New Jersey, Minnesota, Maryland, and Virginia. These payments included retroactive VA disability and VA education benefit payments worth over $150,000. In total, fourteen US Treasury checks were recovered, totaling $572,345.

- The ex-sister-in-law of a deceased veteran was indicted for theft of government funds. An investigation by the VA OIG and Penn Hills Police Department—whose jurisdiction is just outside Pittsburgh—resulted in charges alleging the defendant contacted VA after the veteran's death and redirected two US Treasury checks to her home. The checks were intended for the defendant's niece and nephew, who were the beneficiaries upon the death of her ex-brother-in-law. The defendant allegedly negotiated both checks, totaling approximately $56,000, deposited them into her bank account, and later withdrew the money for her own personal use.

COVID-19 Program Fraud

COVID-19 fraud involves the submission of fraudulent applications for payments under the Small Business Administration's small business pandemic relief programs including the Payroll Protection Program and the Economic Impact Disaster Loan Program. These programs were created through the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which was signed into law in March 2020 in response to the economic fallout from the COVID-19 pandemic.

- A VA OIG investigation resulted in charges alleging that a former VA Outpatient Clinic Health Technician, with the assistance of her church pastor, fraudulently obtained two Paycheck Protection Program loans totaling $49,999. It is further alleged that the pastor and a church deacon fraudulently obtained two Economic Injury Disaster Loans totaling $240,000. The former VA employee previously pleaded guilty to wire fraud, and the deacon pleaded guilty to wire fraud and aiding and abetting wire fraud.

- A former VA medical technician pleaded guilty to wire fraud. A VA OIG investigation revealed that the former VA employee fraudulently obtained $41,666 in Paycheck Protection Program funds and later obtained forgiveness of the loan based on a misrepresentation. The defendant used the fraudulently-obtained funds for personal expenses.

Current number of ongoing investigations: 1,772

Current number of referrals: 775

Audits – Recently Issued Reports and Ongoing Projects

Final Report Published – July 7, 2026: Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement

Patient advocates document interactions with veterans in the Patient Advocate Tracking System-Replacement (PATS-R), which contains personally identifiable and health information that VA is required to protect. The VA OIG conducted this audit to determine whether PATS-R had adequate security controls from March 2025 through January 2026 to safeguard veterans' sensitive information in accordance with federal law and information security standards.

The OIG found that PATS-R received an inappropriate low risk categorization when oversight of the system shifted portfolios in late 2023 and the system migrated to a cloud environment. During the transition, VA's Office of Information and Technology (OIT) did not follow all the steps of the required risk management framework, including revisiting the privacy impact assessment. As a result, the confidentiality, integrity, and availability of veterans' information were put at potential risk. Although OIT updated the system risk categorization to moderate impact in March 2025, access controls still did not function as intended, and the program office did not consistently validate that users were authorized. The OIG also found many users were unaware they could access medical records through PATS-R, and most reported that losing such access would not affect their duties. Additionally, the Office of Patient Advocacy did not provide adequate oversight or guidance to ensure proper role provisioning, account removal, or training updates. Without effective governance and security controls, veterans' sensitive information remained vulnerable to unauthorized access. VA concurred with the OIG's five recommendations.

Final Report Published – July 16, 2026: Review of VA's Compliance with the Payment Integrity Information Act for Fiscal Year 2025

The VA OIG conducted this review to determine whether VA complied with the requirements of the Payment Integrity Information Act of 2019 (PIIA) for fiscal year (FY) 2025. PIIA requires federal agencies to identify, test, report, and remediate risks in programs that may be susceptible to significant improper payments, following Office of Management and Budget (OMB) guidance. It also requires each OIG to review its agency's improper payment reporting and issue an annual report. In FY 2025, VA

reported improper and unknown payment estimates totaling about $3.9 billion across seven programs. Of that amount, approximately $1.5 billion (38 percent) represented a monetary loss, while the other $2.4 billion (62 percent) was considered either a nonmonetary loss that cannot be recovered or an unknown payment. The FY 2025 estimate was about $1.8 billion higher than FY 2024 largely because VA incorporated its largest program, Compensation, into its improper payment estimates for the first time.

The OIG concluded that VA met all six PIIA requirements for FY 2025. All seven programs identified as susceptible to significant improper or unknown payments reported rates below the statutory 10 percent threshold. The Supplies and Materials program reported a rate well below the threshold and is no longer considered high risk; it will undergo risk assessments at least every three years, as required by PIIA. VA also satisfied additional reporting requirements for three high-priority programs—Pension, VA Community Care, and Compensation—by providing quarterly updates to OMB that described actions to prevent and recover monetary losses from improper payments.

The OIG found VA's testing, reporting, and remediation efforts responsive to reducing improper payments. The OIG did not make recommendations in this report.

Final Report Published – July 17, 2026: Denials of Emergency Care Claims

This VA OIG management advisory memorandum notified the under secretary for health that Veterans Health Administration (VHA) claims-processing practices for non-VA emergency care appeared inconsistent with federal law.

The Cleland–Dole Act of 2022 requires third-party organizations seeking reimbursement or direct payment for a veteran's non-VA emergency treatment to file claims within 180 days of the last date of care. Despite this requirement, VHA continued applying an older, 90-day regulatory deadline until October 2025. Although VHA had since updated its internal process, the OIG found that the revised approach—allowing processors to choose between the 90-day and 180-day windows—still did not fully comply with the law.

VHA's Office of Finance identified about 78,000 third-party claims, totaling more than $373 million in billed charges, that were denied under the outdated 90-day deadline after the law changed in December 2022. As of late 2025, these claims had not been reviewed for potential errors, and corrective payments had not been initiated. VHA had begun

work to update relevant regulations but had not completed them as of May 2026, leaving claims adjudication vulnerable to continued inconsistencies.

The OIG concluded that denying third-party claims submitted within the 180-day statutory period appeared inconsistent with the Cleland–Dole Act. The memorandum asked the under secretary for health to review the issues and report any resulting actions. The under secretary acknowledged the findings and stated that VHA was reviewing affected claims, refining internal guidance, and accelerating necessary policy and regulatory updates. The OIG issues advisory memoranda when prompt attention can reduce risks to veterans or prevent significant financial losses.

Final Report Published – July 23, 2026: Review of Open Obligations in VBA's General Operating Expenses Account

The VA OIG reviewed the Veterans Benefits Administration's (VBA) oversight of open obligations—including undelivered orders and unpaid delivered orders (accruals)—from March 1 through May 15, 2025. The review assessed whether VBA effectively managed funds within its $4 billion fiscal year 2025 general operating expenses account, which supports the administration and delivery of veterans' benefits. VA financial policy requires monthly reviews and reconciliation of all open obligations to ensure balances are accurate, documented, and valid. Obligations that are open beyond their period of performance or are inactive for more than 90 days are considered stale and must be reviewed and, when appropriate, deobligated.

The OIG found that VBA did not consistently follow these requirements, delaying the identification and release of funds that could have been redirected to support veterans. From March 1 through May 15, 2025, about 2,200 undelivered orders valued at $1.9 billion were stale. From a statistical sample, the OIG projected that nearly 2,100 of these orders—totaling about $1.7 billion—had not been properly reviewed, and about 1,600 (representing $895.3 million) should have been deobligated but were not. VBA also did not review an estimated 1,000 accruals. Staff relied on an automation in the Integrated Financial and Acquisition Management System rather than verifying expenses and confirming that they aligned with each obligation's period of performance as required.

Contributing factors included outdated guidance that did not reflect current financial systems, insufficient documentation of reviews, and inconsistent communication among finance, requesting, and contracting offices. Leaders noted challenges with staffing and

reliance on legacy systems.

The OIG made three recommendations to improve oversight, strengthen policy compliance, and enhance financial stewardship as VA continues to realign its finance and budget functions.

Final Report Published – July 24, 2026: Review of the Fiduciary Program's Misuse Allegation Process

The VA OIG conducted this review to help protect vulnerable beneficiaries from fiduciaries' misuse of their VA benefits payments. The OIG team examined whether VBA fiduciary program staff took action that was consistent with governing guidance for about 1,600 misuse allegation cases completed from April 2024 through March 2025. Properly recording fiduciaries' potential misuse of beneficiaries' funds and investigating credible allegations against fiduciaries are vital to stopping financial abuse and reimbursing misused VA benefits to beneficiaries.

The OIG found that fiduciary program staff did not always accurately record the earliest date when misuse allegations were received and did not advance all allegations of potential misuse for investigation consistent with requirements. Contributing causes for these issues included staff's confusion about applying unclear provisions from the VA Fiduciary Program Manual and incorrectly applying standards of evidence. The OIG team found there was no systematic national monitoring of misuse allegations to detect staff's missteps. Without clearer guidance about how staff should record and investigate misuse allegations, the risk of financial abuse will continue undetected. In addition, comprehensive oversight of allegations about misuse of funds would provide greater assurance that staff are correctly managing misuse allegations.

The OIG made four recommendations to clarify and improve guidance so allegations about fiduciaries' misuse of benefits are correctly recognized, recorded, processed, and advanced for investigation.

Final Report Published – July 24, 2026: Audit of the Education Service's Compliance Surveys

The VA OIG conducted this audit to determine how VBA manages compliance surveys of education and training institutions that receive VA benefits. These surveys are required by law and help prevent fraud, waste, and abuse. The OIG team reviewed surveys from October 1, 2022, through September 30, 2025 (fiscal years 2023, 2024, and 2025).

The OIG found that during these fiscal years, 646 of the 7,669 institutions (8 percent) with individuals enrolled under Education Service–administered programs that required a compliance survey were not scheduled for one and did not have a waiver excluding them from being scheduled. Therefore, VBA did not meet 38 U.S.C § 3693 statutory requirements for compliance surveys in fiscal years 2023–2025. VBA also did not consider students using benefits under Chapter 31 (Veteran Readiness and Employment) when deciding which institutions needed surveys, even though this is required by law. VBA did not meet the statutory requirement because the Education Service lacked documented or standard processes and procedures to identify institutions and assign surveys.

The OIG also found that survey workload among VBA staff and contractors was uneven, communication between regions was limited, and quality checks on completed surveys were weak. Finally, the OIG found that VBA approved payments to a compliance survey contractor without fully verifying its performance. Because of this, the OIG questioned over $19 million paid to the contractor for fiscal years 2023 through 2025.

Without better processes, there is a continued risk that institutions may receive improper payments or fail to comply with applicable statutes and regulations, increasing the chance of education benefits fraud. The OIG made six recommendations to improve how VBA manages, schedules, and reviews these surveys.

Final Report Published – July 27, 2026: Federal Information Security Modernization Act Audit for Fiscal Year 2025

Agency program officials, chief information officers, and inspectors general must annually review information security programs and report to the Department of Homeland Security and Congress on agency compliance with the Federal Information Security Modernization Act (FISMA). The OIG contracted with an independent public accounting firm, CliftonLarsonAllen LLP (CLA), to evaluate VA's information security program for fiscal year 2025. After assessing 24 major applications and general support systems hosted at 11 VA facilities and on the VA Enterprise Cloud, CLA concluded that VA continues to face significant challenges meeting FISMA requirements because of the nature and maturity of its information security program.

The audit found continuing deficiencies related to access controls, configuration management controls, security management controls, and service continuity practices designed to protect mission-critical systems from unauthorized access, alteration, or

destruction. These deficiencies can be remedied by improving the deployment of security patches, system upgrades, and system configurations; improving performance monitoring to ensure controls operate as intended; and communicating identified security deficiencies to appropriate personnel.

CLA made 19 recommendations, some of which addressed repeat deficiencies from previous FISMA reports over multiple years; two were new recommendations. CLA also closed six previous recommendations due to improvements. VA did not concur with the recommendations. CLA will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions in the fiscal year 2026 audit of VA's information security program.

Current number of ongoing audits and reviews: 48

Current number of ongoing healthcare hotline inspections and national reviews: 31

Fraud Awareness Training

DATE	TOPIC AND LOCATION
7/1/26	Fraud Awareness Brief - Phoenix VARO
7/1/26	Fraud Awareness Brief - VAPD, Minneapolis, MN
7/6/26	Fraud Awareness Brief - VAPD Lovell Federal Healthcare Center, North Chicago, IL
7/14/26	Fraud Awareness Brief - Louisville VAMC
7/16/26	Fraud Awareness Brief - Chicago OHI
7/22/26	Fraud Awareness Brief - West Palm Beach VAMC
7/23/26	Fraud Awareness Brief - West Palm Beach VAMC
7/23/26	Fraud Awareness Brief - Indianapolis VARO
7/29/26	Fraud Awareness Brief - Altoona, PA VAMC