JUNE 2022 HIGHLIGHTS

Congressional Testimony

Testimony before the House Veterans' Affairs Subcommittee on Technology Modernization and Senate Veterans' Affairs Committee Roundtable on Information Technology and Cybersecurity

Mike Bowman, Director of Information Technology and Security in the OIG Office of Audits and Evaluations, testified before the House Veterans' Affairs Subcommittee on Technology Modernization on June 7, 2022. The hearing focused on VA's progress toward implementing a robust cybersecurity program and the difficulties VA faces in adapting its antiquated legacy systems to continuously evolving operational and security requirements. Mr. Bowman discussed the OIG's annual Federal Information Security Modernization Act of 2014 (FISMA) audits, the most recent of which identified repeat findings and deficiencies related to configuration management, identity management and access, and contingency planning controls. He also discussed the OIG's IT security inspection program, which examines sites not evaluated under the annual FISMA audits, and how this and other ongoing oversight efforts can help spur progress, especially if OIG recommendations are proactively reviewed and implemented by IT leaders across the enterprise. A recording of the hearing is available on the committee website. The following day, Mr. Bowman appeared at a Senate Veterans' Affairs Committee roundtable in which participants discussed VA's efforts to bolster its cybersecurity posture and better protect veterans' information. The roundtable, which was not recorded by the committee, also included Office of Information and Technology (OIT) representatives and private sector healthcare company executives who shared their best practices.

Office of Investigations

This office investigates potential crimes and civil violations of law involving VA programs and operations concerning VA employees, contractors, beneficiaries, and other individuals. These investigations focus on a wide range of matters, including healthcare, procurement, benefits, construction, and other fraud; cybercrime and identity theft; bribery and embezzlement; drug offenses; and violent crimes. The following investigations had significant developments this month.

Healthcare Investigations

Physician Charged in Connection with Ordering Unnecessary Tests and Taking Bribes and Kickbacks

A multiagency investigation resulted in charges alleging a physician entered into an improper agreement with a diagnostic imaging company through which he was paid bribes and kickbacks in exchange for ordering unnecessary transcranial doppler tests. He received approximately $148,000 and may have billed the government and private insurance companies as much as $3.25 million in unnecessary tests.

The loss to VA is at least $650,000. The physician was charged in the District of Massachusetts with conspiracy to commit healthcare fraud and conspiracy to violate the Anti-Kickback Statute. The investigation was conducted by the VA OIG, FBI, IRS Criminal Investigation (CI), Department of Health and Human Services (HHS) OIG, US Postal Inspection Service, and Department of Labor Employee Benefits Security Administration.

Business Owner Pleaded Guilty for Role in Fraud Scheme Involving COVID-19 and Cancer Genetic Testing

A Georgia man who owned and operated a marketing company that generated leads for medical testing companies participated in a conspiracy to defraud federally funded and private healthcare benefits programs. From 2019 to 2020, he and his coconspirators provided testing companies with patient leads for medically unnecessary cancer genetic screening tests in exchange for kickbacks of approximately $1,000 to $1,500 for each test that resulted in a reimbursement from Medicare. The business owner fabricated a contract and invoices to make it appear as though he was being paid for legitimate services and to conceal the kickback scheme. In March 2020, he began receiving kickbacks on a per-test basis for COVID-19 tests, provided that those tests were bundled with a much more expensive respiratory pathogen panel test, which does not identify or treat COVID-19. The defendant pleaded guilty in the District of New Jersey to conspiracy to violate the Anti-Kickback Statute and conspiracy to commit healthcare fraud. The loss to VA is approximately $330,000. The VA OIG, Defense Criminal Investigative Service, FBI, IRS CI, and HHS OIG conducted this investigation.

Pharmaceutical Executive Charged for Conspiring to Sell Excessively Priced COVID-19 Personal Protective Equipment to VA

According to another multiagency investigation, an executive for a pharmaceutical secondary wholesaler conspired with others to defraud at least a dozen VA medical centers by selling personal protective equipment at excessive prices during the COVID-19 pandemic. The executive allegedly used deceitful means to sell the equipment to VA, which totaled $330,000. He was charged in the Southern District of Mississippi with conspiracy to defraud the United States. The investigation was conducted by the VA OIG, FDA Office of Criminal Investigations, and FBI.

Former VA Registered Nurse Pleaded Guilty for COVID-19 Vaccination Card Fraud Scheme

A former registered nurse at the John D. Dingell VA Medical Center in Detroit, Michigan, stole authentic COVID-19 vaccination record cards from the facility, as well as the vaccine lot numbers necessary to make the cards appear legitimate. She then resold the cards and lot numbers for $150–$200 each to individuals within the metropolitan Detroit area. The defendant pleaded guilty in the Eastern District of Michigan to theft of government property. The VA OIG worked with the HHS OIG and VA Police Service to investigate this case.

Marine Veteran Charged for Using Stolen Identity and Allegedly Receiving VA Benefits

A multiagency investigation resulted in charges alleging that a presumed Mexican national stole the

identity of a deceased American teenager to enlist in the US Marine Corps in the 1970s. Despite having no legal basis for living or working in the United States, he served for approximately three years on active duty under the assumed identity and, in 2021, allegedly received VA education and medical benefits and applied for VA disability benefits. The defendant was arrested after being charged in the Southern District of California with identity theft and making false statements related to health care in his application for a passport and in his application for Social Security. The investigation was conducted by the VA OIG, Social Security Administration OIG, Diplomatic Security Service, and California Department of Motor Vehicles.

Veteran Charged for Firing a Weapon Outside VA Medical Facility

A veteran discharged a 12-gauge shotgun outside the Ravenna VA Clinic in Ohio. The defendant was near the flagpole in front of the clinic entry, and after being approached by a security guard, he allegedly displayed the shotgun and discharged a shell into the ground. The VA clinic and a nearby school and private hospital were immediately locked down. After discussions with a SWAT team negotiator, the veteran ultimately surrendered and was later indicted in the Portage County (Ohio) Court of Common Pleas for inducing panic and possession of criminal tools, with firearms specifications. The VA OIG, Ravenna Police Department, and VA Police Service conducted the investigation.

Veteran Pleaded Guilty to Making Threats to Clinic and Help Line Personnel

VA OIG investigators determined that a veteran repeatedly made vulgar and threatening comments to staff at the Lake Jackson VA Outpatient Clinic in Texas, the Veterans Crisis Line, and the White House VA Hotline. The veteran pleaded guilty in the Southern District of Texas to making threats by interstate communications.

Veteran Indicted for Making Threats against VA Doctors

A veteran allegedly called the White House VA Hotline and threatened to harm doctors at the Fargo VA Medical Center in North Dakota. The veteran was indicted in the District of North Dakota for communicating interstate threats. The VA OIG, VA Police Service, and US Marshals conducted this investigation.

Veteran Charged for Making Threats against VA Boston Healthcare Director and Subsequently Threatening to Kill VA OIG Agents

A VA OIG and VA Police Service investigation resulted in charges alleging a veteran threatened to harm the director of the VA Boston Healthcare System during a telephone call to the facility. While the veteran was under investigation for making these threats, he allegedly called VA Police Service and threatened to kill the VA OIG agents who were attempting to interview him. He was arrested and charged in Brockton District Court (Massachusetts) with threatening to commit murder.

Benefits Investigations

Veteran Sentenced for Theft of Government Benefits and False Statements

A VA OIG investigation found that a veteran fraudulently led VA to believe he was blind. The veteran, who had been receiving service-connected disability benefits at a 100 percent rating since June 2011, falsely stated to VA that he was unable to drive and had someone drive for him. Despite these claims, he possessed a valid driver's license with a motorcycle endorsement and drove on a routine basis. After previously being found guilty by a federal jury on charges of theft of government property and false statements, the veteran was sentenced in the Middle District of Florida to 27 months in prison, two years of supervised release, and more than $429,000 in restitution to VA.

Former VA Fiduciary Charged with Misappropriation

According to an investigation by the VA OIG, a former VA-appointed fiduciary illegally spent over $115,000 in VA compensation benefits intended for her veteran uncle. The former fiduciary allegedly used the stolen funds as a down payment for a home and to pay for subsequent home improvement projects. She was charged in the Eastern District of Louisiana with misappropriation by a fiduciary.

Investigations Involving Other Matters

Mortgage Lender Agreed to Pay More than $1 Million to Resolve Fraud Allegations

A VA OIG and HUD OIG investigation resolved allegations that a mortgage lender improperly and fraudulently originated government-backed mortgage loans insured by the Federal Housing Administration (FHA). According to the investigation, the lender knowingly underwrote FHA mortgages and approved for insurance mortgages that did not meet FHA requirements or qualify for insurance, resulting in losses to the federal government when the borrowers defaulted on those mortgages. It was further alleged that the lender knowingly failed to perform required quality control reviews. VA paid more than $1.2 million in claims for loans originated by this defendant. The mortgage lender entered into a civil settlement agreement in the Eastern District of Washington under which it agreed to pay more than $1 million to resolve these allegations.

Nonveteran Found Guilty for Role in Service-Disabled Veteran-Owned Small Business Fraud Scheme

Two nonveterans fraudulently created a service-disabled veteran-owned small business (SDVOSB) by installing a service-disabled veteran as the ostensible owner of the business, which remained under their control. Over 10 years, the SDVOSB was awarded more than $305 million in government contracts. Of this amount, approximately $77 million was awarded by VA, including a $24 million set-aside contract to build a parking garage at the VA Long-Term Spinal Cord Injury Clinic in Dallas, Texas. One of the nonveterans was found guilty at trial in the Western District of Texas of conspiracy to defraud the United States and wire fraud. The other nonveteran, as well as the veteran, previously pleaded guilty in connection with this investigation.

Office of Audits and Evaluations

The Office of Audits and Evaluations (OAE) provides independent oversight of VA's activities to improve the integrity of its programs and operations. This work helps VA improve its program results, promotes economy and efficiency, strengthens controls over the delivery of benefits, identifies potential fraud, verifies compliance with laws and regulations, and enhances veteran care and support. OAE released the following reports this month.

Featured Report

Suicide Prevention Coordinators Need Improved Training, Guidance, and Oversight

As part of the Veterans Health Administration's (VHA) suicide prevention strategy, suicide prevention coordinators at VA medical facilities are required to reach out to veterans referred from the Veterans Crisis Line. Coordinators facilitate access to assessments, interventions, and effective care; encourage veterans to seek care, benefits, or services from VA or in the community; and follow up to connect veterans with appropriate care and services after the call.

The VA OIG conducted a review to evaluate whether coordinators properly managed crisis line referrals to ensure at-risk veterans were being reached. The review team found that coordinators mistakenly closed some veteran referrals due to inadequate training, guidance, and oversight necessary to maximize chances of reaching at-risk veterans referred by the crisis line. VHA's Office of Mental Health and Suicide Prevention is responsible for issuing policy and guidance for managing crisis line referrals.

VHA also lacked comprehensive performance metrics to assess coordinators' management of crisis line referrals, which was particularly important because coordinators lacked clear guidance on managing crisis line referrals. Until VHA provides appropriate training, issues adequate guidance, and improves performance metrics, coordinators could miss opportunities to reach and assist at-risk veterans. The OIG made five recommendations that include improving data integrity, training coordinators on using patient outcome codes, developing additional guidance, monitoring compliance with requirements to space calls over three days, and evaluating program data for additional opportunities to improve services for referred veterans. The under secretary for health concurred or concurred in principle with all the report's findings and recommendations and submitted action plans for recommendations 1 through 5.

Publications on Healthcare Access and Administration

VA Medical Facilities Took Steps to Safeguard Refrigerated Pharmaceuticals but Could Further Reduce the Risk of Loss

VA reportedly lost about $1.1 million in January 2019 because medical facilities failed to maintain

appropriate storage temperatures for refrigerated pharmaceuticals, prompting VHA to issue requirements about responsibilities, processes, and procedures for safeguarding them. The OIG conducted an audit to determine if VA medical facilities met those requirements and found they generally stored the drugs safely. VA medical facilities reported about $1.7 million in losses for fiscal year (FY) 2021 out of about $1.4 billion spent on refrigerated pharmaceuticals, which the OIG acknowledges is relatively minimal. Pharmacy Benefits Management Services officials agreed that medical facility officials should strengthen and reinforce safeguards to further reduce the risks of loss or of veterans receiving compromised medications or vaccines. The OIG recommended the under secretary for health reinforce requirements for storing refrigerated pharmaceuticals and establish a procedure to help ensure medical facilities comply with VHA Notice 2021-16, "Storage of Vaccines and Medications in Pharmaceutical Grade Purpose-Built Refrigerators and Freezers at VA Medical Facilities." Guidance should also be updated to clarify that medical facilities must report all refrigerated pharmaceutical loss.

Publication on Benefits Delivery and Administration

Contract Medical Exam Program Limitations Put Veterans at Risk for Inaccurate Claims Decisions

The VA OIG reviewed the Veterans Benefits Administration's (VBA's) contract medical disability exam program and found VBA's governance of and accountability for the program needs to improve. Limitations with VBA's management and oversight of the program at the time of the review caused identified deficiencies to persist. VBA should improve the program to help ensure vendors produce accurate exams to support correct decisions for veterans' claims. Some of the vendors' exams have not met contractual accuracy requirements. As a result, processors may have used inaccurate or insufficient medical evidence to decide veterans' claims, which can be minimized through improved governance and accountability measures. The OIG made four recommendations, including ensuring vendors can be held contractually accountable for unsatisfactory performance and establishing procedures for vendors to correct errors. The OIG also recommended VBA's Medical Disability Examination Office improve its process to communicate errors and analyze all available data to identify systemic errors and trends.

Publications on Finance

Financial Efficiency Review of the VA El Paso Healthcare System in Texas and New Mexico

This review assessed the oversight and stewardship of funds by the VA El Paso Healthcare System and identified potential cost efficiencies in carrying out medical center functions. The following financial activities and administrative processes were examined to determine whether the healthcare system had appropriate oversight processes and controls for open obligations, purchase card use, Medical/Surgical Prime Vendor–Next Generation program use, and pharmacy operations. The review team identified several opportunities for the healthcare system to improve oversight and ensure the appropriate use of funds. The OIG made 12 recommendations to the VA El Paso Healthcare System director to use as a

road map to improve financial operations. The recommendations address issues that, if left unattended, may interfere with effective financial efficiency practices and the strong stewardship of VA resources.

Results of Consulting Engagement Related to Selected Financial Reporting Controls for the Integrated Financial and Acquisition Management System at the National Cemetery Administration

The VA OIG contracted with the independent public accounting firm CliftonLarsonAllen LLP (CLA) to provide consulting services to the OIG with respect to selected financial reporting controls for the Integrated Financial and Acquisition Management System (iFAMS) at the National Cemetery Administration (NCA). VA is implementing iFAMS using an incremental approach, with the first deployment having occurred at NCA in November 2020. The nature and scope of work were determined solely by agreement between the OIG and CLA and did not constitute an audit. In its consulting letter, CLA provided the OIG with observations and potential risks in such categories as obligations, reconciliations, opening balances, procurement, and intragovernmental transactions. The OIG shared this letter with VA management officials for their awareness.

A Summary of Preaward Reviews of VA Federal Supply Schedule Pharmaceutical Proposals Issued in Fiscal Year 2021

The OIG reviews pharmaceutical proposals submitted to the VA National Acquisition Center for Federal Supply Schedule contracts valued annually at $5 million or more. The reviews are not published because they contain sensitive commercial information protected from release under the Trade Secrets Act. This report, however, summarizes the 15 preaward reviews of the pharmaceutical proposals that the OIG conducted in FY 2021. The 15 proposals had a cumulative 10-year estimated contract value of about $8.3 billion and included 846 offered drug items. The review team concluded that commercial disclosures were accurate, complete, and current for four of the 15 proposals reviewed. The remaining 11 proposals could not be reliably used for negotiations until the noted deficiencies were corrected. The OIG made recommendations for lower prices than offered for 10 of the 15 proposals, resulting in the Acquisition Center awarding contracts or modifications with cost savings of about $42.6 million.

Review of VA's Compliance with the Payment Integrity Information Act for FY 2021

The Payment Integrity Information Act of 2019 requires federal agencies to review all programs and activities they administer that may be susceptible to significant improper payments based on Office of Management and Budget guidance. The OIG reviewed whether VA complied with the law in FY 2021 and found that VA reported improper and unknown payment estimates totaling $5.12 billion for seven programs and activities. Though VA had an overall decrease in total improper payments and unknown payments, the overall monetary loss more than doubled from $892 million in FY 2020 to $1.97 billion. Though VA satisfied nine of the law's 10 requirements, it failed to report an improper and unknown payment rate of less than 10 percent for four programs and activities that had estimates in materials accompanying their financial statements. The OIG recommended the under secretary for health reduce improper and unknown payments to below 10 percent for those noncompliant programs.

Publications on Information Technology

Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Dallas, Texas

The OIG conducts IT inspections to assess whether VA facilities are meeting federal security requirements. They are typically conducted at selected facilities that have not been assessed in the annual FISMA audit or at facilities that previously performed poorly. The OIG selected the Dallas Consolidated Mail Outpatient Pharmacy (CMOP) because it had not been previously visited as part of the OIG's annual FISMA audit. The inspections focus on configuration management, contingency planning, security management, and access controls. The OIG found deficiencies in configuration management and access controls, but none in contingency planning or security management controls. The OIG made 10 recommendations to the Dallas CMOP director intended to fix the control deficiencies. The assistant secretary for information and technology provided comments for the Dallas CMOP. The assistant secretary concurred with nine recommendations but did not concur with one recommendation to implement an effective vulnerability and flaw remediation program. The nonconcurrence was attributed to OIT being able to demonstrate vulnerability identification, remediation, mitigation, and management rates of 96 percent for all critical and high vulnerabilities at the Dallas CMOP. However, the OIG found there was a lack of evidence to support that assertion and stands by its recommendation.

Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona

The OIG also conducted an IT inspection of the Tucson CMOP and found that the pharmacy had inaccurate component inventories, ineffective vulnerability management, and inadequate flaw remediation; had not implemented the configuration management plan; lacked a disaster recovery plan; had not changed the default username and password for the security camera system; and did not consistently generate or forward audit records. Without these controls, critical systems may be at risk of unauthorized access or destruction. The OIG made six recommendations to the Tucson CMOP director: implement (1) effective inventory management tools, (2) an effective vulnerability and flaw remediation program, and (3) a disaster recovery plan; (4) ensure CMOP staff understand their roles and responsibilities; (5) task the facility manager with changing the default username and password for the security camera system; and (6) ask OIT to configure audit logging.

Veterans Data Integration and Federation Enterprise Platform Lacks Sufficient Security Controls

VA is required by law to ensure veterans' sensitive personal information is safely shared across a highly fragmented healthcare system. The OIG audited whether OIT developed and implemented the Veterans Data Integration and Federation Enterprise Platform's (VDIF) security controls to ensure confidentiality, data integrity, and the safeguarding of sensitive health information according to federal standards. The OIG found OIT let VDIF become operational without effectively executing all required risk

management framework steps. OIT inappropriately categorized some security objectives (resulting in 22 important controls not being applied) and did not adequately determine whether the implemented controls were correctly applied. Because of insufficient oversight, VDIF became operational with inadequate security controls, heightening the risk to personal health information within more than 10 million veteran records. VA did not concur with OIG recommendations to reestablish VDIF to ensure appropriate high-level controls but agreed to more effectively oversee establishing and monitoring security controls to ensure proper processes are followed.

Mission Accountability Support Tracker Lacked Sufficient Security Controls

Following a May 2021 hotline complaint, the OIG evaluated the merits of an allegation that VBA disregarded privacy procedures so it could more quickly use a workload tracking system without receiving the appropriate security authorization. The Mission Accountability Support Tracker (MAST) helps quantify the work VBA staff do in response to employee requests for support services. Staff enter personally identifiable information (PII) into the system, which could be compromised in an unauthorized, unsecure application. The OIG found that VBA and OIT did not correctly assess the privacy impact, misclassified MAST, and lacked authority to operate MAST before using it. The report's four recommendations included ensuring future IT projects follow an approved management process and providing sufficient guidance to staff to ensure MAST is used as intended, while keeping the PII of VA employees and contractors safe and secure.

Office of Healthcare Inspections

The Office of Healthcare Inspections (OHI) assesses VA's efforts to maintain a fully functional healthcare program that promotes high-quality patient care and safety and prevents adverse events. Staff conduct inspections prompted by OIG hotline complaints, congressional requests, and other leads. The office also performs inspections of vet centers and individual medical centers, healthcare systems, networks, and community providers. OHI released the following reports this month.

Healthcare Inspections

Deficits with Metrics Following Implementation of the New Electronic Health Record at the Mann-Grandstaff VA Medical Center in Spokane, Washington

The OIG evaluated the availability and utilization of metrics more than a year after the Mann-Grandstaff VA Medical Center became the first VHA medical center to implement the new electronic health record (EHR) system. With VA's transition to the new EHR, metrics were created by adding new EHR data to the existing VA data repository and by using the new EHR's functionality. The OIG found that gaps in available metrics due to the new EHR transition impaired the facility's ability to measure and act on issues of organizational performance, quality of care and patient safety, and access to healthcare services. The OIG is concerned that further deployment of the new EHR without addressing these issues may impede the ability of the facility and future sites to provide timely, effective, safe, and veteran-

centered care. The OIG made two recommendations to the deputy secretary related to evaluating gaps in new EHR metrics and the factors affecting the availability of metrics and taking action as warranted.

Multiple Failures in Test Results Follow-up for a Patient Diagnosed with Prostate Cancer at the Hampton VA Medical Center in Virginia

This inspection assessed concerns related to facility providers' failures to communicate, act on, and document abnormal test results that led to a delay in a patient's diagnosis of prostate cancer. The patient, a male in his 60s, was diagnosed with metastatic prostate cancer in April 2021. In July 2019, a vascular surgeon failed to communicate and act on an abnormal computerized tomography (CT) scan. In fall 2020, a primary care provider failed to communicate test results to the patient and to act on an abnormal prostate-specific antigen test result. The primary care provider also failed to correctly enter bone scan orders, and a technologist incorrectly attempted to correct this error. Consequently, the notification for the results, showing diffuse metastatic bone disease, were not sent to a provider. Finally, facility leaders did not initiate quality reviews as required by VHA policy. The OIG made seven recommendations to the facility director related to test results, clarity in urology consults, nuclear medicine orders, patient safety reporting, and initiation of quality management reviews.

Failure of Leaders to Address Safety, Staffing, and Environment of Care Concerns at the Tuscaloosa VA Medical Center in Alabama

The VA OIG assessed allegations at the Tuscaloosa VA Medical Center that facility and community living center (CLC) leaders failed to address CLC safety and security issues, and that facility leaders failed to fill key positions, utilize unused space, and ensure the environment of care and grounds provided a safe setting. The OIG found that facility leaders failed to address CLC safety and security issues and to fill several key positions, but did not substantiate that they failed to use available space to provide care for patients or ensure the environment of care and grounds provided a safe setting. The OIG made one recommendation to the Veterans Integrated Service Network (VISN) director to ensure completion of VISN site visit recommendations. Nine recommendations were made to the facility director related to assessing CLC security; developing a plan for the coverage, recruitment, and retention of difficult-to-fill positions; and improving facility environmental care rounds.

Pharmacists' Practices Delayed Buprenorphine Refills for Patients with Opioid Use Disorder at the New Mexico VA Health Care System in Albuquerque

This inspection assessed allegations at the New Mexico VA Health Care System regarding the policy and practices related to buprenorphine treatment for patients with an opioid use disorder. The OIG substantiated that pharmacists declined early refills based on a policy not applicable to buprenorphine treatment for opioid use disorder. The Opioid Safety Committee pharmacist was found to have placed standing orders for urine drug screening, which the scope of practice allowed. The OIG did not substantiate that the Opioid Safety Committee chairperson interfered with prescribing providers' practices, that the buprenorphine standing operating procedure (SOP) was inconsistent with VHA guidance, that practices varied from VHA guidance on increasing buprenorphine access, or that leaders

failed to respond to a provider's patient safety concerns. Five recommendations were made to the facility director to align early buprenorphine refill practices with policy, communicate about early medication refills, educate staff about the Opioid Safety Committee, revise the buprenorphine SOP to ensure it is consistent with evidence-based treatment, and review provider staffing.

Comprehensive Healthcare Inspections

Comprehensive Healthcare Inspection Program (CHIP) reports are one element of the OIG's overall efforts to ensure that the nation's veterans receive high-quality and timely VA healthcare services. The inspections are performed approximately every three years for each facility. The OIG selects and evaluates specific areas of focus on a rotating basis. See the Purpose and Scope section of each report for the areas of focus at the time of the inspection:

The OIG published the following CHIP reports this month for these facilities and systems:

Hershel "Woody" Williams VA Medical Center in Huntington, West Virginia

Beckley VA Medical Center in West Virginia

VA Maryland Health Care System in Baltimore

Washington DC VA Medical Center

***

To listen to the podcast on the June 2022 highlights, go to www.va.gov/oig/podcasts.