Inspector General
U.S. Department of Defense

January 2021

Newsletter



Recently Issued Reports (to view report, if available, please click on title)

Audit of Infectious Disease Medical Treatment Capabilities at Al Udeid Air Base

This audit determined that the 379th Expeditionary Medical Group had the capabilities to treat patients infected with COVID-19 and isolate or quarantine suspected infected service members, civilians, and contractors. The 379th EMDG developed response plans, established procedures to screen Al Udeid Air Base personnel attempting to enter medical treatment facilities, and initiated COVID-19 testing. Additionally, the 379th Expeditionary Medical Group increased its on-hand inventory of personal protective equipment and acquired COVID-19 testing kits to detect infected service members, civilians, and contractors. As a result, the 379th Expeditionary Medical Group was able to quickly identify COVID-19 patients, expedite restriction of movement measures, and conduct contact tracing to prevent the spread of the virus throughout Al Udeid Air Base.

Audit of the Disinfection of Department of Defense Facilities in Response to the Coronavirus Disease-2019 Pandemic

This audit determined that for the 21 cases at eight DoD installations we reviewed from April 1, 2020 through June 30, 2020, DoD and contractor personnel disinfected areas occupied by individuals who tested positive for COVID-19 in accordance with the Centers for Disease Control guidance. As a result, DoD personnel reduced the risk of exposure to COVID-19 and protected DoD personnel from the spread of COVID-19 in DoD workspaces.

Special Report: Weaknesses in the Retrograde Process for Equipment from Afghanistan

This report highlights weaknesses related to property accountability, security, and contractor oversight of retrograde operations of equipment in Afghanistan identified in previous DoD Office of Inspector General reports issued between 2013 and 2015. These reports identified weaknesses that significantly impacted the

retrograde process, such as a lack of recurring inventories that contributed to the accumulated loss of $586.8 million in equipment, inaccurate accountability and visibility of equipment, and lack of security and safeguarding of sensitive items that left equipment and information vulnerable to theft and compromise.

Audit of the Department of Defense's Compliance With the Berry Amendment

This audit determined that while the Military Services and the Defense Logistics Agency generally complied with the Berry Amendment for DoD procurements and acquisitions, opportunities exist to increase compliance and consistency in the implementation of Berry Amendment requirements throughout the pre-award, award, and administration phases of the contracting process. The Berry Amendment promotes the purchase of goods manufactured in the United States by directing how the DoD can use funds to purchase end items (fabrics, food, and hand tools) over the simplified acquisition threshold of $250,000. However, the Military Services and Defense Logistics Agency contracting officials issued solicitations for 9 of 74 contracts, valued at $7 million, without the required Berry Amendment Defense Federal Acquisition Regulation Supplement (DFARS) clauses; awarded 6 of 135 contracts, valued at $14 million, without the required Berry Amendment DFARS clauses; and as a result of our audit they modified an additional 11 of 135 contracts, valued at $14.3 million, to include the required Berry Amendment DFARS clauses. Additionally, Defense Contract Management Agency officials did not document the Berry Amendment as an item for administration for 26 of 44 contracts reviewed, valued at $796.6 million. As a result, the Military Services, the Defense Logistics Agency, and the Defense Contract Management Agency have limited assurance that items procured and delivered were in compliance with the Berry Amendment.

Summary of Reports Issued Regarding Department of Defense Cybersecurity Issued From July 1, 2019 through June 30, 2020

This report summarized the results of 44 DoD cybersecurity-related reports issued by the DoD Office of Inspector General, Government Accountability Office, and other DoD oversight organizations from July 1, 2019 through June 30, 2020. This summary report determined that DoD Components implemented corrective actions necessary to close 197 of the 656 cybersecurity-related recommendations included in this summary report and prior summary reports. Those corrective actions indicate progress in the DoD's efforts to mitigate or remediate risks and weaknesses to the DoD systems and networks. However, as of August 2020, the DoD still had 459 cybersecurity-related recommendations that remained open, with some recommendations dating back to 2011. Despite improvements made by the DoD, cybersecurity reports issued during the last year demonstrate that the DoD continues to face significant challenges in managing cybersecurity risks to its systems and networks.

Audit of the Department of Defense's Implementation of Section 3610 of the Coronavirus Aid, Relief, and Economic Security Act

This audit determined that in general, DoD contracting officers complied with the Office of Management and Budget and DoD guidance to support rational decisions that were in the best interest of the Government when approving requests related to section 3610 of the Coronavirus Aid, Relief, and Economic Security Act. Section 3610 of the Act, authorized agencies to reimburse contractors for any paid leave, including sick leave, they provide to keep their employees or subcontractor employees in a "ready state." This includes protecting the life and safety of Government and contractor personnel. However, the DoD faced some challenges implementing section 3610 that extended beyond the audit sample, such as contracting officers having to rely on the contractor's self-certification of the use of other COVID–19 relief measures, tracking and identifying section 3610 in DoD contracts, and the lack of a specific appropriation for section 3610.

Recently Issued Reports (cont'd)

Evaluation of Defense Logistics Agency Contracts for Ventilators in Response to the Coronavirus Disease-2019 Outbreak

This evaluation determined that the Defense Logistics Agency took proactive measures to acquire ventilators by contacting six vendors already on contract in response to COVID-19. The Defense Logistics Agency took initiative to acquire ventilators prior to receiving customer requests due to projected national shortages. As a result, the Defense Logistics Agency's actions reduced delivery delays, which could have resulted from a high demand for ventilators in the fight against the COVID-19 disease.

External Peer Review of the Defense Finance and Accounting Service Internal Review Audit Function

This external peer review, for the period ending June 30, 2020, determined that the system of quality control for the Defense Finance and Accounting Service Internal Review (IR) audit organization was suitably designed and complied with to provide the Defense Finance and Accounting Service Internal Review audit organization with reasonable assurance of performing and reporting in conformity in all material respects with applicable professional standards. Audit organizations can receive a rating of pass, pass with deficiencies, or fail. The Defense Finance and Accounting Service Internal Review audit organization received a rating of pass.

System Review Report on the Defense Information Systems Agency Office of Inspector General Audit Organization

This system review, for the period ending May 31, 2020, determined that the system of quality control for the Defense Information Systems Agency Office of Inspector General (OIG) audit organization was suitably designed and complied with to provide the Defense Information Systems Agency OIG audit organization with reasonable assurance of performing and reporting in conformity in all material respects with applicable professional standards. Audit organizations can receive a rating of pass, pass with deficiencies, or fail. The Defense Information Systems Agency OIG audit organization received a rating of pass.

Review of the Department of Defense's Implementation of Executive Order 13950, Combating Race and Sex Stereotyping, September 22, 2020

This evaluation reviewed and assessed DoD compliance with the requirements of Executive Order 13950, "Combating Race and Sex Stereotyping," and focused on DoD compliance with agency requirements of sections 3 through 7 of the executive order. This evaluation determined that the DoD is in compliance with the requirements in sections 3 and 5 of Executive Order 13950, and is making progress toward implementing the requirements of sections 6 and 7. However, the DoD did not fully comply with section 4, which requires Federal agencies to include a contract provision in all Government contracts issued on or after November 21, 2020. Based on the non-statistical sample of 21 DoD contracts issued from November 23, 2020, through December 1, 2020, 19 of 21 contracts did not contain the required contract provision.

Upcoming Reports

Significant reports expected to be issued within the next 30 days include:

Audit of Dual-Status Commanders for Use in Defense Support of Civil Authorities Missions

This audit determines whether DoD Components nominated, certified, and appointed dual-status commanders for Defense Support of Civil Authorities missions in accordance with legal authorities and DoD policies in response to the COVID–2019 pandemic (COVID-19).

Audit of Depot-Level Reparable Items at Tobyhanna Army Depot

This audit determines whether Army officials considered and mitigated challenges to parts availability when planning and executing repair and overhaul of reparable items for command, control, computers, communications, cyber, intelligence, surveillance, and reconnaissance at the Tobyhanna Army Depot.

Interagency Coordination Group of Inspectors General for Guam Realignment Annual Report for Fiscal Year 2020

This report describes the obligations, expenditures, and revenues associated with military construction on Guam, in response to the FY 2010 National Defense Authorization Act. Section 2835 of the Act established the Interagency Coordination Group of Inspectors General for Guam Realignment and requires an annual report summarizing—for the preceding calendar year—the activities under programs and operations funded with amounts appropriated, or otherwise made available for, military construction on Guam.

Audit of the Defense Logistics Agency's Sole Source, Captains of Industry Strategic Support Contracts

This audit determines whether the Defense Logistics Agency's sole source, Captains of Industry strategic support contracts are achieving cost savings, value, and benefits for the DoD. Captains of Industry strategic support contracts use performance-based outcomes to provide increased warfighter support to improve the availability of spare parts and order response time, reduce repair turn-around time, improve reliability and maintenance planning, and augment repair capability. These contracts have overarching terms and conditions to support innovation, cost reduction, and responsiveness; long-term commitments; and the ability to expand beyond parts support including service-driven requirements, engineering improvements, life cycle management support, and remanufacturing or repair.

Evaluation of the U.S. Combatant Commands' Responses to the Coronavirus Disease–2019 Pandemic (U.S. Central Command)

This evaluation determines how Geographic Combatant Commands (excluding U.S. Northern Command) and their component commands, executed their pandemic response plans. The evaluation also focuses on challenges with implementing the response plans and the impact the COVID-19 pandemic had on operations. This report focuses on U.S. Central Command and is the third report in a series of reports on the Combatant Commands.

Upcoming Reports (cont'd)

Evaluation of the Aircraft Monitor and Control System's Nuclear Certification

This evaluation between the DoD Office of Inspector General and the Department of Energy Office of Inspector General determines whether testing conducted on the Aircraft Monitor and Control system for the DoD's nuclear weapon capable delivery aircraft meets the DoD and Department of Energy's nuclear certification requirements. This evaluation was conducted in conjunction with the Department of Energy Office of Inspector General, which will issue a separate report on matters related to the Department of Energy.

Evaluation of Department of Defense Contracting Officer Actions on Questioned Direct Costs

This evaluation determines whether the actions taken by DoD contracting officers on questioned direct costs reported by the Defense Contract Audit Agency are in compliance with Federal regulations, and DoD and agency policy.

External Peer Review of the Defense Contract Audit Agency

The objective of this review is to determine, for the period ending June 30, 2019, whether the quality control program for the Defense Contract Audit Agency was designed and complied with to provide reasonable assurance that the Defense Contract Audit Agency and its personnel performed audits and reported in conformity with applicable professional standards.

Audit of Cybersecurity Requirements for Department of Defense Weapons Systems in the Operation and Support Phase of the Acquisition Process

This audit determines whether DoD Components took action to update cybersecurity requirements for weapon systems in the operations and support phase of the acquisition lifecycle, based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats**. This report is classified.**

Audit of Cybersecurity Controls Over the Air Force Satellite Control Network

This audit determines whether the U.S. Space Force implemented cybersecurity controls to protect the Air Force Satellite Control Network against potential threats. **This report is classified.**

Defense Criminal Investigative Service Highlights

Acting Manhattan U.S. Attorney Announces $40.5 Million Settlement with Durable Medical Equipment Provider Apria Healthcare for Fraudulent Billing Practices

On December 18, 2020, a U.S. District judge in New York City, New York, approved a $40.5 million settlement of a fraud lawsuit against Apria Healthcare Group, Inc. and its affiliate, Apria Healthcare LLC, a large durable medical equipment provider with approximately 300 branch offices located throughout the United States. The lawsuit alleges that Apria submitted false claims to Federal health programs, including Medicare and Medicaid, seeking reimbursement for the rental of costly non-invasive ventilators ("NIVs") to program beneficiaries who were not using them. Additionally, Apria improperly billed Federal health programs for certain NIV rentals which were being used for treatments that were already available from a less expensive device known as variable positive airway pressure respiratory assistance devices. The company also improperly waived co-pays for a number of Medicare and TRICARE beneficiaries to induce them to rent NIVs. Apria submitted thousands of false claims to Federal health programs for NIV rentals and fraudulently received millions of dollars in reimbursements. This was a joint investigation with the Defense Criminal Investigative Service (DCIS), the Department of Health and Human Services Office of Inspector General (OIG), and the Office of Personnel Management OIG.

International Trio Indicted in Austin for Illegal Exports to Russia

On December 18, 2020, the U.S. Attorney's Office in Austin, Texas, announced a Federal grand jury indictment had been unsealed charging three foreign nationals with violating the International Emergency Economic Powers Act, Export Control Reform Act, and money laundering statutes in a scheme to procure sensitive radiation-hardened circuits from the United States and ship those components to Russia through Bulgaria without required licenses. According to the indictment, Russian national Ilias Sabirov, and Bulgarian nationals Dimitar and Milan Dimitrov used Bulgarian company Multi Technology Integration Group EEOD to receive controlled items from the United States and send them to Russia. Under U.S. export control law, the goods could not be shipped to Russia without the permission of the U.S. Government. In addition, the defendants and their companies have been designated by the Department of Commerce as persons who present a greater risk of diversion to weapons of mass destruction programs, terrorism or other activities contrary to U.S. national security or foreign policy interests. This was a joint investigation with DCIS, the Federal Bureau of Investigation (FBI), and the Department of Commerce Office of Export Enforcement.

Defendants and Pharmacies Admit to Executing Health Care Fraud Schemes Targeting Veterans

On December 11, 2020, in Pittsburgh, Pennsylvania, brothers Mehran David Kohanbash and Joseph Kohan, and their nephew Nima Rodefshalom, pleaded guilty in Federal court to charges of health care fraud, conspiracy to commit fraud, and conspiracy to violate the Federal anti-kickback statutes. In addition, 16 pharmacies in California, Texas, Wyoming, Arizona, and Nevada also entered guilty pleas for their roles in the three individual defendants' scheme. According to the Government, the three defendants conspired together to execute health care fraud schemes that targeted patients of bariatric surgical procedures. They, together with the defendant pharmacies, engaged in a misleading advertising campaign that resulted in the defendants obtaining patients' insurance information. The defendants subsequently solicited patients to appeal to their respective physicians to prescribe expensive medications that were often compounded, resulting in high profits for the individuals and pharmacies. The defendants also defrauded multiple healthcare benefit programs—including TRICARE—

by manipulating the collection of co-pays on various medications to make it appear that they were being collected when, in fact, they were not. An honest reporting of the failure to collect co-pays would have resulted in the defendants being unable to bill insurance carriers for the cost of the various medications. This was a joint investigation with DCIS and the FBI.

Defense Contractors Charged and Sentenced for Turkey-Based Defense Contracting Fraud Scheme

On December 11, 2020, in Atlanta, Georgia, multiple defense contractors were charged or sentenced for participating in a multimillion-dollar defense contracting fraud scheme based out of Turkey. According to the U.S. Attorney's Office for the Northern District of Georgia, Murat Gonenir, with at least two other defendants, participated in an extensive Turkey-based scheme to defraud the U.S. military. The defendants applied for and obtained access to a sensitive DoD contracting database housing some of the military's most sensitive schematics. Gonenir obtained access to this sensitive database by falsely claiming he was a U.S. or Canadian citizen or permanent resident. The defendants then offered bids on numerous defense contracts for these sensitive schematics that required them to produce these parts in the United States. Instead, they produced these parts in Gonenir's manufacturing plants in Turkey and then falsely claimed to the DoD that the parts had been lawfully produced in the United States. The DoD paid millions to the various defense contractors who took part in this scheme as a result of these false statements. Three defendants were sentenced to terms of imprisonment ranging from 6 to 41 months and ordered to pay approximately $1.75 million in combined restitution. This was a joint investigation with DCIS, the FBI, and the Department of Commerce-Bureau of Industry and Security.

Fraudsters Who Stole Protected Health Information to Fund Spending Spree Plead Guilty

On December 7, 2020, in Sherman, Texas, Demetrius Cervantes, Lydia Henslee, and Amanda Lowry pleaded guilty to conspiracy to obtain information from a protected computer in the Eastern District of Texas. Cervantes, Lowry, and Henslee are alleged to have breached a health care provider's electronic health record system in order to steal protected health information and personally identifiable information belonging to patients. This stolen information was then "repackaged" in the form of fraudulent physician orders and subsequently sold to durable medical equipment providers. Within approximately eight months, the defendants obtained more the $1.4 million in proceeds from the sale of the stolen information. In addition, the defendants are alleged to have conspired to pay and receive kickbacks in exchange for orders from physicians that were subsequently used to obtain payments from federal health care programs. Through this scheme, the conspirators collectively obtained more than $2.9 million. The defendants used the proceeds to purchase assets subject to seizure, including SUVs, off-road vehicles, and jet skis. If convicted, the defendants each face up to five years in Federal prison. This was a joint investigation with DCIS, the Department of Health and Human Services OIG, and the Internal Revenue Service Criminal Investigation Division.

Announced Projects (to view the announcement letters, if available, please click on the title)

Oversight of the Audit of the FY 2021 Army Working Capital Fund Financial Statements

The objective of this oversight project is to provide contract oversight of KPMG's audit of the Army Working Capital Fund Financial Statements for the fiscal years ending September 30, 2021, and September 30, 2020, and determine whether KPMG complied with applicable auditing standards.

Oversight of the Audit of the FY 2021 Army General Fund Financial Statements

The objective of this oversight project is to provide contract oversight of KPMG's audit of the Army General Fund Financial Statements for the fiscal years ending September 30, 2021, and September 30, 2020, and determine whether KPMG complied with applicable auditing standards.