Report No. DODIG-2023-067

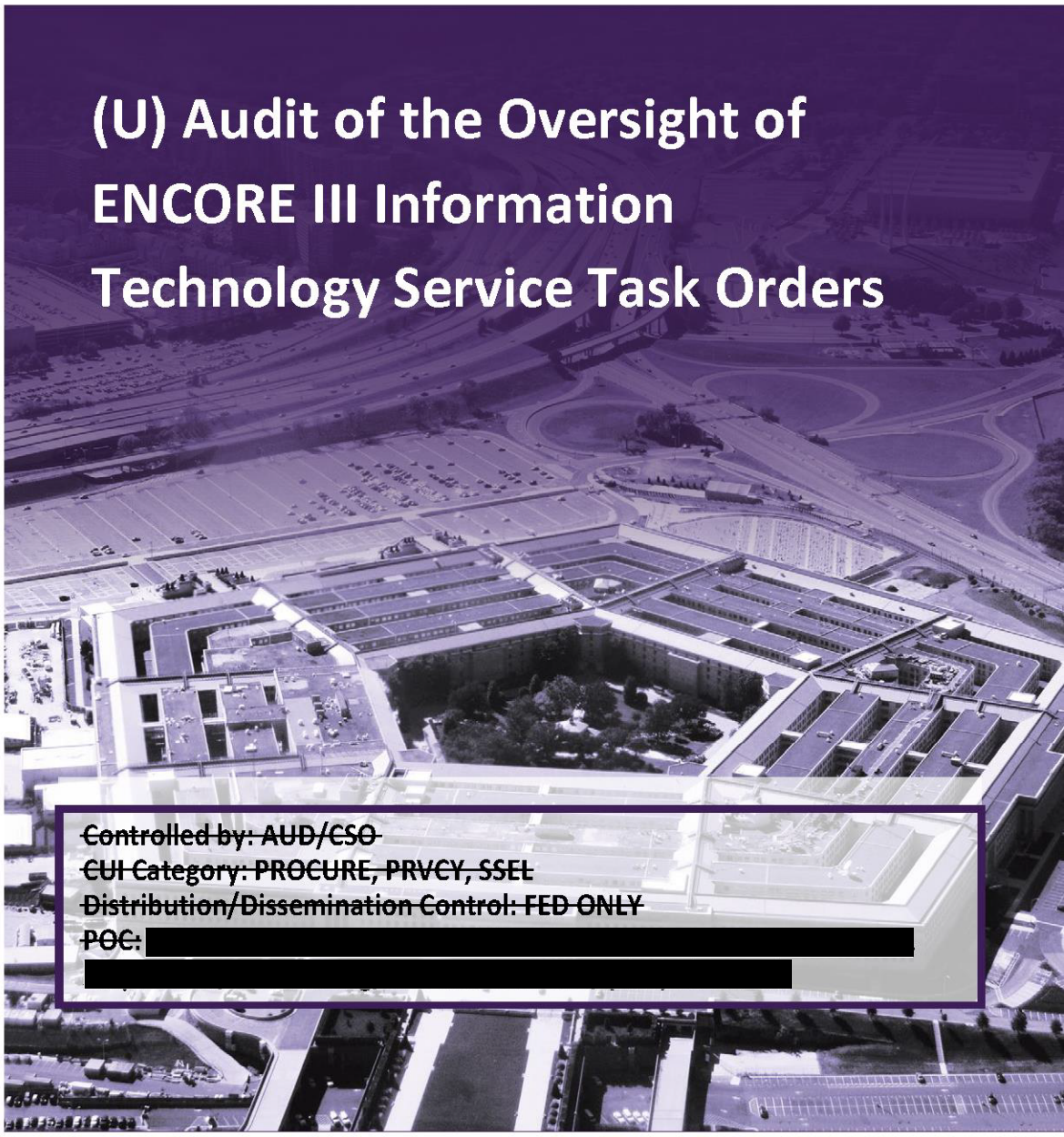
~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

MAY 4, 2023

(U) Audit of the Oversight of ENCORE III Information Technology Service Task Orders



~~Controlled by: AUD/CSO~~
~~CUI Category: PROCURE, PRVCY, SSEL~~
~~Distribution/Dissemination Control: FED ONLY~~
~~POC:~~ [redacted]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

~~CUI~~

(U) Results in Brief

(U) Audit of the Oversight of ENCORE III Information Technology Service Task Orders

(U) May 4, 2023

(U) Objective

(U) The objective of this audit was to determine whether DoD Components performed oversight of task orders issued under the Defense Information Systems Agency's (DISA) ENCORE III information technology service contract in accordance with Federal and DoD guidance. We reviewed a sample of five task orders awarded by DISA, U.S. Transportation Command (USTRANSCOM), and Washington Headquarters Services (WHS) contracting officers.

(U) Finding

(U) DoD Component contracting officer's representatives (COR) did not oversee contractor performance in accordance with Federal and DoD guidance for the ENCORE III task orders we reviewed. Specifically, the CORs did not consistently maintain documentation of inspections of contractor performance, submit timely surveillance reports to contracting officers, or review contractor interim vouchers to prevent improper payments.

(U) This occurred because contracting officers were not required to review COR files to determine whether the CORs were performing their duties as required until the CORs had been in place for 1 year. Our results indicate that waiting a year to review COR files is insufficient to detect and correct COR performance problems in a timely manner. In addition, COR training did not include instruction on how to review interim vouchers to prevent improper payments.

(U) Furthermore, six of the eight CORs for the ENCORE III task orders did not meet technical experience requirements to oversee the contractor cybersecurity services required by the task orders. This occurred because three of the five requiring activities did not nominate qualified officials to be CORs, and the contracting (U) officers did not verify that the COR nominees possessed the technical experience needed to oversee cybersecurity services before designating them as CORs. As a result, the CORs relied on other officials to inspect contractor performance, which violated DoD guidance and increased the risk of the DoD paying for services not received.

(U) The lack of COR oversight for the ENCORE III task orders resulted in the DoD officials paying $24.2 million without reasonable assurance that contractor information technology services met task order requirements.

(U) Recommendations

(U) Among other recommendations, we recommend that the Principal Director of Defense Pricing and Contracting (DPC) revise DoD guidance to require contracting officers to conduct initial reviews of COR files within a set timeframe from designating CORs. We also recommend that the Principal Director develop and implement plans to ensure contracting officers are aware of the technical experience requirements for CORs who monitor cybersecurity services. We recommend that the Defense Acquisition University (DAU) President revise the DoD COR training to include detailed instructions for CORs to review interim vouchers to prevent improper payments.

(U) Management Comments and Our Response

(U) The Principal Director of DPC, the DAU Chief of Staff, and other management officials generally agreed with 14 of our 19 recommendations; however, 5 recommendations remain unresolved. We request additional comments on the unresolved recommendations within 30 days. Please see the Recommendations Table on the next page for the status of the recommendations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Principal Director of Defense Pricing and Contracting, Office of the Under Secretary of Defense for Acquisition and Sustainment	4.a.1, 4.a.2, 4.a.3	4.b, 4.c, 4.d, 4.e	None
Defense Acquisition University President	None	5	None
Defense Information Systems Agency Head of the Contracting Activity	1.c	1.a, 1.b, 1.d, 1.e	None
U.S. Transportation Command Head of the Contracting Activity	None	2.a, 2.b, 2.c, 2.d	None
Washington Headquarters Services Head of the Contracting Activity	3.a	None	3.b (U)

(U) Please provide Management Comments by June 5, 2023.

(U) The following categories are used to describe agency management's comments to individual recommendations:

- (U) **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- (U) **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- (U) **Closed** – DoD OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

May 4, 2023

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT
COMMANDER, U.S. TRANSPORTATION COMMAND
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES

SUBJECT: (U) Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Report No. DODIG-2023-067)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains five recommendations that are considered unresolved because management officials did not fully address the recommendations presented in the report. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations remain open. We will track these recommendations until an agreement is reached on the actions that need to be taken to address the recommendations, and management officials submit adequate documentation showing that all agreed-upon actions are completed.

(U) This report contains 13 recommendations that are considered resolved. Therefore, as described in the Recommendations, Management Comments, and Our Response section of this report, we will close the recommendations when we receive adequate documentation showing that all agreed-upon actions to implement the recommendation are completed.

(U) This report contains one recommendation that is considered closed because management officials took action to address the recommendation.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, within 30 days please provide us your comments concerning specific actions in process or alternative corrective actions proposed on the recommendations. Please send your comments to audcso@dodig.mil. For the resolved recommendations, within 90 days please provide us documentation showing you have completed the agreed-upon actions. Please send your documentation as a PDF to followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

(U) Responses must have the actual signature of the authorizing official for your organization.

(U) If you have any questions or would like to meet to discuss the audit, please contact me at [redacted]. We appreciate the cooperation and assistance received during the audit.

FOR THE INSPECTOR GENERAL:

Carol N Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations & Acquisition,
Contracting, and Sustainment

(U) Contents

(U) Introduction

(U) Objective 1

(U) Background 1

(U) Review of Internal Controls 6

(U) Finding. DoD Component CORs Did Not Properly Oversee the ENCORE III Task Orders 7

(U) DoD Component CORs Did Not Properly Oversee Contractor Performance 8

(U) Contracting Officers Did Not Review COR Files in a Timely Manner 13

(U) DoD COR Training Did Not Include Instruction on Interim Voucher Reviews 14

(U) CORs Did Not Meet Technical Experience Requirements to Oversee Cybersecurity Services 15

(U) The DoD Paid $24.2 Million Without Reasonable Assurance That Contractor Information Technology Services Met Task Order Requirements 18

(U) Other Matters of Interest 18

(U) Management Comments on the Finding and Our Response 19

(U) Recommendations, Management Comments, and Our Response 20

(U) Appendixes

(U) Appendix A. Scope and Methodology 30

- (U) Internal Control Assessment and Compliance 32
- (U) Use of Computer-Processed Data 32
- (U) Use of Technical Assistance 32
- (U) Prior Coverage 32

(U) Appendix B. Contracting and Requiring Activities Reviewed 33

(U) Appendix C. Summary of the Notice of Concern, DISA Comments, Our Response, and DISA Actions Taken 35

- (U) Notice of Concern 36
- (U) Management Comments 38

(U) Appendix D. Summary of Potential Monetary Benefits 40

- (U) Management Comments on the Potential Monetary Benefits and Our Response 40

(U) Management Comments

(U) Defense Contracting and Pricing 42

(U) Defense Acquisition University 44

(U) Defense Information Systems Agency 45

(U) U.S. Transportation Command 49

(U) Washington Headquarters Services 52

(U) DoD Chief Information Officer 59

(U) Acronyms and Abbreviations 60

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether DoD Components performed oversight of task orders issued under the Defense Information Systems Agency's (DISA) ENCORE III information technology services contract in accordance with Federal and DoD guidance.[1] See Appendix A for a discussion of the scope and methodology.

(U) Background

(U) The ENCORE III information technology services contract provides DoD and Federal agencies with a wide range of services to support information technology development, installation, operation, and management. DISA initially awarded the ENCORE III contract on November 2, 2017, as a multiple-award, task-order contract valued up to $17.5 billion with a maximum period of performance of 10 years.[2] As of March 31, 2022, DoD contracting activities had issued 48 task orders against the ENCORE III contract with a combined value of $1.6 billion. Contracting activities can award ENCORE III task orders using any combination or variation of fixed-price or cost-reimbursable contract types. Fixed-price contracts require contractors to deliver supplies or services for pre-determined prices. Cost-reimbursable contracts require the U.S. Government to pay contractor expenses incurred for delivering supplies or services.

(U) Federal and DoD Contract Oversight Guidance

(U) The Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) are the primary Federal and DoD guidance for quality assurance and the oversight of contracts. FAR part 46 states that agencies must ensure that supplies and services acquired under U.S. Government contracts conform to the contract's quality and quantity requirements and include inspection, acceptance, and other measures associated with quality requirements.[3] DFARS part 246 requires DoD Components to implement a contract quality assurance program to ensure that contract performance conforms to specified requirements.[4] DFARS subpart 246.4 states that contracting officers for service contracts should prepare quality assurance surveillance plans to facilitate assessment of contractor performance.[5]

---

[1] (U) Federal Acquisition Regulation Part 2, "Definitions of Words and Terms," identifies a task order as an order for services placed against an established contract or with U.S. Government sources.

[2] (U) A multiple-award contract is a type of contract that contracting officers award to at least two contractors.

[3] (U) FAR Part 46, "Quality Assurance."

[4] (U) DFARS Part 246, "Quality Assurance."

[5] (U) DFARS Part 246, "Quality Assurance," Subpart 246.4, "Government Contract Quality Assurance."

(U) The DFARS Procedures, Guidance, and Information (PGI) contains implementing guidance for the DFARS. DFARS PGI subpart 201.6 requires contracting officers to designate officials as contracting officer's representatives (COR) to assist them with overseeing DoD service contracts.[6]

(U) COR Identification, Designation, and Responsibilities

(U) DoD Instruction 5000.72 establishes standards for identifying and designating CORs and defines general COR responsibilities.[7] DoD Instruction 5000.72 also states that requiring activities should nominate officials who have completed COR training and are qualified by education, training, and experience to oversee the services procured under a specific contract.[8] The Instruction requires contracting officers to review the COR nominees' qualifications and either accept or reject the nominees based on meeting education, training, and experience requirements. Furthermore, the Instruction requires contracting officers to issue designation letters to CORs to specify the roles and responsibilities that the contracting officers delegate to the CORs, which may include:

- (U) monitoring contractor performance to ensure that the contractor meets the contract terms, conditions, and specifications;
- (U) inspecting contractor deliverables to determine whether they satisfy contract requirements;
- (U) preparing and submitting surveillance reports on contractor performance matters to the contracting officer; and
- (U) reviewing interim vouchers to ensure that contractor expenses are commensurate with contractor work performed for cost-reimbursable services.

(U) For each assigned contract, a COR must maintain a surveillance file in the Procurement Integrated Enterprise Environment (PIEE) System.[9] The surveillance file must contain a copy of the COR designation letter, other documents describing the

[6] (U) DFARS PGI Part 201, "Federal Acquisition Regulation System," Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities." DFARS PGI subpart 201.6 exempts a contracting officer from designating CORs for a service contract when the requirement is not complex, the contract is awarded using simplified acquisition procedures, and the contracting officer documents why a COR is not needed.

[7] (U) DoD Instruction 5000.72, "DoD Standard for Contracting Officer's Representative (COR) Certification," March 26, 2015 (Incorporating Change 1, August 31, 2018). On November 6, 2020, the Under Secretary of Defense for Acquisition and Sustainment updated DoD Instruction 5000.72 with administrative changes.

[8] (U) See also DoD Instruction 5000.74, "Defense Acquisition of Services," January 10, 2020, which identifies that a requiring activity is a DoD Component, or part of a DoD Component, that identifies and defines a requirement for supplies or services, and requests the initiation of, and provides funding for, a contract to fulfill the requirement.

[9] (U) The DoD's PIEE System provides end-to-end procurement capabilities and business processes, from the decision to procure supplies or services until contract close-out.

(U) COR's duties and responsibilities, and documentation of inspections and surveillance performed. The contracting officer is required to review the COR file annually in the anniversary month of the COR's designation to ensure that the COR is performing delegated responsibilities and maintaining accurate and complete records.

(U) Task Orders Reviewed

(U) We reviewed a nonstatistical sample of 5 ENCORE III task orders, valued at $279.8 million, from the universe of 25 ENCORE III task orders that were ongoing as of March 31, 2020. We selected our sample based on the total dollar value of the task orders, the task order type, and the period of performance. Contracting officers from DISA, the U.S. Transportation Command (USTRANSCOM), and Washington Headquarters Services (WHS) awarded the five ENCORE III task orders in support of the Joint Staff; Commander, Navy Installations Command (CNIC); Joint Service Provider (JSP); the Program Executive Office USTRANSCOM (PEO–T); and the Pentagon Force Protection Agency (PFPA).[10]

(U) On November 8, 2021, a DISA contracting officer modified one of the five ENCORE III task orders to change the requiring activity from the Joint Staff to the 318th Cyberspace Operations Group, a U.S. Air Force Air Combat Command (ACC) unit. Therefore, we refer to this task order as the ACC Task Order throughout this report. See Table 1 for the task orders selected for review. Descriptions of each of the task orders follow the table. See Appendix B for descriptions of the contracting activities and the requiring activities responsible for the task orders.

(U) Table 1. Task Orders Selected for Review

(U) Contracting Activity	Requiring Activity	Task Order	Award Date	Total Value at Award
DISA	ACC*	HC1028-19-F-6100	1/30/2019	**$27,519,809**
DISA	CNIC	HC1028-19-F-6320	9/27/2019	**116,174,220**
DISA	JSP	HC1028-19-F-6101	9/26/2019	**73,996,274**
USTRANSCOM	PEO–T	HTC711-20-F-D012	11/27/2019	**17,083,856**
WHS	PFPA	HQ0034-19-F-0486	7/31/2019	**45,004,556**
Total				**$279,778,715 (U)**

*(U) The Joint Staff was the requiring activity on the task order award date, but the requiring activity changed to the ACC during our audit.
(U) Source: The DoD Office of Inspector General (OIG).

[10] (U) The Defense Information Technology Contracting Organization, USTRANSCOM Directorate of Acquisition, and the WHS Acquisition Directorate are the DISA, USTRANSCOM, and WHS contracting activities, respectively. Throughout the report, we refer to contracting officers from these organizations as DISA, USTRANSCOM, and WHS contracting officers.

(U) ACC Task Order

(U) A DISA contracting officer awarded the ACC Task Order on January 30, 2019, to support the Joint Staff Deputy Directorate for Joint Training's planning and execution of up to 1,500 cyber, electronic warfare, and information operations training events per year on the Joint Information Operations Range. The contractor is responsible for supporting the planning of the training events, developing the system security plan, reviewing interconnection security agreements, and conducting cyberspace defense for the Joint Information Operations Range. The task order includes a base year and four option years with a total value of $27.5 million, and the contracting officer exercised the third option year to extend the task order through May 31, 2023.

(U) On November 8, 2021, a DISA contracting officer modified the task order to change the requiring activity from the Joint Staff Deputy Directorate for Joint Training to the ACC 318th Cyberspace Operations Group, as authorized by the Under Secretary of Defense for Personnel and Readiness and in accordance with a memorandum of agreement between the Joint Staff and the U.S. Air Force.[11]

(U) Commander, Navy Installations Command Task Order

(U) A DISA contracting officer awarded the CNIC Task Order on September 27, 2019, to support the operation of the CNIC Fleet and Family Readiness Directorate's Enterprise Military Housing System, which provides services for Army, Marine Corps, Navy, Air Force, Space Force, and Coast Guard personnel to obtain housing at military installations throughout the world. The contractor is responsible for maintaining and sustaining information technology capabilities and functions associated with the system, providing customer service for DoD housing officials who need assistance using the system, and ensuring that the system complies with Federal, DoD, and Navy technical and cybersecurity policies. The task order includes a base year and four option years with a total value of $116.2 million, and the contracting officer exercised the third option year to extend the task order through September 29, 2023.

(U) Joint Service Provider Task Order

(U) A DISA contracting officer awarded the JSP Task Order on September 26, 2019, to support the cybersecurity of hundreds of information systems operated by the Office of the Secretary of Defense, the Joint Staff, and DoD agencies, including the DoD OIG.[12] The contractor was responsible for assisting the JSP Cyber Security Center in reviewing security authorization packages, assessing cyber risks, and identifying and managing vulnerabilities for information systems. The task order included a 5-month base period

[11] (U) "Memorandum of Agreement Between the Joint Staff and the United States Air Force for Joint Information Operations Range Mission and Resource Transition," January 9, 2020.

[12] (U) See Appendix A for information on DoD OIG operations related to the JSP Task Order.

(U) with three option years, for a total value of $74 million, and the contracting officer exercised two of the three option years.

~~(CUI)~~ During the audit, we issued a notice of concern to alert the DISA Director that JSP officials were proposing a [redacted] modification to the JSP Task Order that might be out of scope of the task order, which would violate the competition requirements of section 2304, title 10, United States Code. Consistent with the suggested action from our notice of concern, the contracting officer allowed the task order to expire on February 24, 2022, without making the modification. See Appendix C for a summary of the notice of concern, comments from DISA's Assistant to the Director, our response, and the DISA contracting officer's actions taken.

(U) Program Executive Office USTRANSCOM Task Order

(U) A USTRANSCOM contracting officer awarded the PEO–T Task Order on November 27, 2019, to support the operation and enhancement of USTRANSCOM's Integrated Data Environment and Global Transportation Network Convergence System, which provides the capability to track DoD cargo and passengers throughout the world.[13] The contractor is responsible for ensuring that the system is available for use; for developing, testing, and implementing software improvements; and for ensuring that the system complies with Federal and DoD cybersecurity policies. The task order includes a 10-month base period and four option years for a total value of $17.1 million, and the contracting officer exercised the third option year to extend the task order through September 30, 2023.

(U) Pentagon Force Protection Agency Task Order

(U) A WHS contracting officer awarded the PFPA Task Order on July 31, 2019, to support PFPA Security Integration and Technology Directorate systems that are critical to the security of the Pentagon and other DoD facilities in the National Capital Region.[14] The contractor was responsible for developing system improvements, performing system administration, and ensuring that the systems complied with Federal and DoD cybersecurity policies. The task order included an 11-month base period and four option years for a total value of $45 million, but the WHS contracting officer did not exercise any of the option years and allowed the PFPA Task Order to expire on June 30, 2020.

[13] (U) USTRANSCOM designated the contractor's services as operationally critical support that is essential to the mobilization, deployment, and sustainment of U.S. Armed Forces engaged in contingency operations.

[14] (U) See Appendix A for information on DoD OIG operations related to the PFPA Task Order.

(U) Review of Internal Controls

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[15] We identified internal control weaknesses with DoD COR designation and oversight processes. We will provide a copy of the report to the senior officials responsible for internal controls at the Office of the Under Secretary of Defense for Acquisition and Sustainment, DISA, USTRANSCOM, and WHS.

[15] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013 (Incorporating Change 1, June 30, 2020).

(U) Finding

(U) DoD Component CORs Did Not Properly Oversee the ENCORE III Task Orders

(U) The DoD Component CORs did not oversee contractor performance in accordance with Federal and DoD guidance for the five ENCORE III task orders we reviewed. Specifically, the CORs did not:

- (U) consistently maintain documentation of inspections of contractor performance in the COR files for all five task orders,
- (U) submit timely surveillance reports to the contracting officers for four task orders,
- ~~(CUI)~~ [redacted], or
- (U) review contractor interim vouchers to prevent improper payments for four task orders.

(U) This occurred because contracting officers did not review COR files to determine in a timely manner whether the CORs performed all duties in the designation letters. At the time of our audit, the CORs for the ENCORE III task orders had been in place for less than a year, and therefore, the contracting officers were not yet required to review the COR files. Our results show that waiting a year to review COR files is insufficient oversight to detect and correct COR performance problems in a timely manner. In addition, COR training did not include instruction on how to review interim vouchers to prevent improper payments.

(U) Furthermore, six of the eight CORs for the ENCORE III task orders did not meet technical experience requirements to oversee the contractor cybersecurity services required by the task orders. This occurred because three of the five requiring activities did not nominate qualified officials to be CORs, and the contracting officers did not verify that the COR nominees possessed the technical experience needed to oversee cybersecurity services before designating them to perform COR responsibilities. Therefore, the CORs relied on other requiring activity officials to inspect contractor performance, which violated DoD guidance. Having a COR accept the contractor's work for payment without being directly involved in monitoring contractor performance increases the risk to the DoD of paying for services not received.

(U) The lack of COR oversight for the five ENCORE III task orders resulted in DoD officials paying $24.2 million without reasonable assurance that contractor information technology services met task order requirements, including $167,335 of travel costs that may not have been reasonable, allowable, or supported by records.

(U) DoD Component CORs Did Not Properly Oversee Contractor Performance

~~(CUI)~~ The DoD Component CORs did not oversee contractor performance in accordance with Federal and DoD guidance for the five ENCORE III task orders we reviewed. Specifically, the CORs did not consistently maintain inspection results in the COR file, submit timely surveillance reports to contracting officers, [redacted], or review interim vouchers to prevent improper payments.

(U) CORs Did Not Consistently Document Inspections of Contractor Performance

(U) The CORs for all five task orders stated that they conducted inspections of contractor performance throughout the period of our review, but none were consistently documenting those inspections in the COR files. The designation letters require the CORs to conduct inspections to ensure that contractors perform in accordance with the requirements, terms, and conditions of the ENCORE III task orders and maintain records of the inspections and the inspection results in their COR files. To determine whether the CORs documented their inspection results in their COR files, we requested and reviewed the COR files from November 2019 through April 2020 for all five task orders.

(U) The CORs for the five ENCORE III task orders did not consistently document contractor performance inspections in their COR files. Specifically, the CORs for the ACC and PEO–T Task Orders maintained spreadsheets to track deliverables but did not document details of inspections and inspection results, and the CORs for the CNIC and PFPA Task Orders acknowledged that they did not have detailed inspection records. The CORs for the JSP Task Order had a memorandum of record to document a series of inspections from January and February 2020, but that record primarily focused on the contractor's administrative errors, such as incorrect grammar in written deliverables, instead of on whether contractor performance satisfied task order requirements. CORs provided various reasons for their inconsistent documentation, such as a lack of time or lack of awareness of recordkeeping requirements.

(U) COR inspections of contractor performance provide the basis for determining whether a contractor satisfied contract requirements and when completing past

(U) performance evaluations.[16] The inspection records also provide the support for taking actions to remedy a contractor's inadequate performance, if necessary.[17] The lack of inspection records reduces the ability of the contracting officer to protect U.S. Government interests when imposing a remedy and in the event of a dispute between the U.S. Government and the contractor. Therefore, the DISA and USTRANSCOM Heads of the Contracting Activity should establish controls to ensure that the contracting officers for the ACC, CNIC, and PEO–T Task Orders monitor whether the CORs are completing inspections and maintaining records of those inspections in the COR surveillance files in the PIEE System.[18]

~~(CUI)~~ *CORs Did Not Submit Timely Surveillance Reports or* [redacted]

~~(CUI)~~ The CORs did not submit timely surveillance reports to the contracting officers for the ACC, CNIC, JSP, and PEO–T Task Orders or [redacted]. DoD Instruction 5000.72 requires CORs to submit surveillance reports to communicate information about contractor performance to contracting officers. To determine whether the CORs prepared and submitted timely surveillance reports on contractor performance, we reviewed COR designation letters and surveillance reports from November 2019 through April 2020, and we interviewed the contracting officers and CORs. Table 2 shows the COR reporting requirements and the frequency with which CORs actually submitted surveillance reports.

[16] (U) A past performance evaluation is the contracting officer and COR's annual report on contractor performance in satisfying contract requirements. Contracting officers review past performance evaluations to make contract award decisions. Despite the lack of inspection records, the contracting officers and CORs completed past performance evaluations for the ENCORE III task orders reviewed.

[17] (U) A remedy is an action taken to safeguard the U.S. Government's interests and minimize the impact of contractor performance problems on the contract. Remedies can include actions such as issuing a cure notice requiring the contractor to "cure" its failure or failures, or reducing or denying award fees. If the non-compliance is persistent, the remedy could be contract termination.

[18] (U) We did not make recommendations to the DISA and WHS Heads of the Contracting Activity for the JSP and PFPA Task Orders because those task orders expired.

(U) Table 2. COR Reporting Requirements and How Often CORs Submitted Surveillance Reports

(U) Task Order	Contracting Activity	COR Reporting Requirement in Designation Letter	How Often CORs Submitted Reports
ACC	DISA	Monthly	Quarterly
CNIC	DISA	Monthly	Never
JSP	DISA	Monthly	Never
PEO–T	USTRANSCOM	No Requirement	Never
PFPA	WHS	Annually	Once (U)

(U) Source: The DoD OIG.

(U) Surveillance reports provide a basis for communicating interim contractor performance or identified problems. Although the CORs for the CNIC and JSP Task Orders did not submit surveillance reports, the CORs stated that they communicated regularly with their contracting officers about contractor performance matters. The CORs for the ACC Task Order stated that they had competing operational priorities, so they did not have time to submit surveillance reports each month. In response to our audit, the CORs for the ACC Task Order began submitting monthly surveillance reports starting in May 2020. The CORs for the CNIC Task Order also began submitting surveillance reports, but not monthly. Therefore, the DISA Head of the Contracting Activity should direct the contracting officer for the CNIC Task Order to establish controls to verify that the CORs submit surveillance reports in the PIEE System in accordance with their designation letters.[19]

~~(CUI)~~ The COR for the PFPA Task Order complied with his designation letter requirement to submit an annual surveillance report, but the report identified [redacted].[20] Upon reviewing the surveillance report for the PFPA Task Order, the contracting officer [redacted].[21] Had the COR been required to submit a

[19] (U) We did not make a recommendation to the DISA Head of the Contracting Activity for the JSP Task Order because the task order expired.

[20] ~~(CUI)~~ [redacted]

[21] ~~(CUI)~~ [redacted] the contracting officer allowed the PFPA Task Order to expire on June 30, 2020.

~~(CUI)~~ surveillance report more often than annually [redacted].[22]

(U) Conversely, the contracting officer for the PEO–T Task Order did not require the COR to submit surveillance reports in the COR's designation letter. It is critical that contracting officers establish periodic reporting requirements for COR surveillance reports in designation letters. During the audit, the USTRANSCOM contracting officer replaced the COR and issued a new COR designation letter that required annual surveillance reports. However, CORs need to notify contracting officers about contractor performance problems immediately because many remedies are time sensitive and delays in notifying the contracting officer may result in harm to the U.S. Government and limit the types of remedies available. To ensure that contracting officers identify potential performance problems in a timely manner, CORs should submit surveillance reports more than once annually. The USTRANSCOM and WHS Heads of the Contracting Activity should revise the USTRANSCOM and WHS contracting regulations to require contracting officers to establish in COR designation letters that CORs must submit surveillance reports more than once annually.

(U) CORs Did Not Review Contractor Interim Vouchers

(U) The CORs for the ACC, CNIC, JSP, and PFPA Task Orders did not review contractor interim vouchers as required by their designation letters.[23] Specifically, the designation letters required the CORs to determine the validity of contractor expenses, such as travel costs, and notify their contracting officers of any expenses that appeared improper. To determine whether CORs reviewed contractor interim vouchers to prevent improper payments, we interviewed the CORs and reviewed the interim vouchers to determine whether the contractors submitted supporting records for all $167,335 in travel costs as required by the ENCORE III contract. The contractors submitted supporting records for only $7,348 of the $167,335 in travel costs.

(U) Based on the lack of submitted records, we coordinated with the contracting officers and CORs to obtain additional supporting records from the contractors for $78,132 in travel costs. In total, we reviewed $85,480 of the $167,335 in travel costs that the contractors submitted from November 2019 through April 2020.[24] We determined that the DoD reimbursed the contractors for at least $24,905 in travel costs that did not

[22] ~~(CUI)~~ [redacted]

[23] (U) The contractor for the PEO–T Task Order did not submit interim vouchers or otherwise request reimbursement of expenses from November 2019 through April 2020.

[24] (U) We did not review labor hours billed because only one of the five contractors submitted interim vouchers with labor hours billed on a cost-reimbursable basis from November 2019 through April 2020. The other four contractors submitted invoices for firm-fixed-price services during the period we reviewed.

(U) appear reasonable, allowable, or supported as required by FAR 31.201.[25] For example, contractors received reimbursement for airfare costs in excess of the lowest price available, such as first-class airfare, without justifications required by FAR 31.205-46.[26] Similarly, contractors received reimbursement for local travel costs that were prohibited by the ENCORE III contract. Table 3 shows the travel costs that we reviewed and questioned.

(U) Table 3. Summary of Travel Costs Reviewed and Questioned

(U) Task Order	Contracting Activity	Total Travel Costs	Travel Costs Reviewed	Questioned Travel Costs
ACC	DISA	$34,670	$34,670	$2,595
CNIC	DISA	122,143	40,288	11,788
JSP	DISA	3,174	3,174	3,174
PFPA	WHS	7,348	7,348	7,348
Total		**$167,335**	**$85,480**	**$24,905 (U)**

(U) Source: The DoD OIG.

(U) According to a DISA contracting officer, they were not concerned that the CORs did not review the contractor expenses because they assumed that Defense Contract Audit Agency (DCAA) auditors would review the interim vouchers, question discrepancies, and deny payments for expenses not supported by records.[27] However, according to DCAA policy officials, CORs are responsible for reviewing interim vouchers as a first-line review because DCAA auditors review only limited samples of interim vouchers and audit statistical samples of high-risk expenses from all contracts and orders that a contractor has with the DoD. Accordingly, DCAA auditors did not review any of the contractor expenses from November 2019 through April 2020 for the task orders we reviewed.

(U) During the audit, the WHS contracting officer took immediate action to investigate $7,322 of the $7,348 in travel costs we questioned for the PFPA Task Order. The WHS contracting officer confirmed that the travel costs were unallowable and recovered $7,322 from the contractor. Therefore, to ensure that any additional improper payments are recovered, the DISA and WHS Heads of the Contracting Activity should direct the contracting officers for the ACC, CNIC, JSP, and PFPA Task Orders to

[25] (U) FAR Part 31, "Contract Cost Principles and Procedures," Subpart 31.2, "Contracts with Commercial Organizations," Section 31.201, "General." FAR 31.201 states that a contractor must have records that demonstrate an expense was reasonable, allowable, and incurred for the contract in accordance with Federal, DoD, and contract requirements.

[26] (U) FAR Part 31, "Contract Cost Principles and Procedures," Subpart 31.2, "Contracts with Commercial Organizations," Section 31.205, "Selected Costs," Subsection 31.205-46, "Travel Costs."

[27] (U) DCAA auditors are the authorized representatives of contracting officers for approving interim vouchers for payment. DCAA auditors may audit and review contractor records to determine whether to approve, suspend, or disapprove the reimbursement of contractor expenses claimed on interim vouchers.

(U) review the contractors' claimed travel costs of $167,335 and recover from the contractor any costs that were not reasonable, allowable, or supported. See Appendix D for a summary of the potential monetary benefits associated with the review of the travel costs.

(U) Contracting Officers Did Not Review COR Files in a Timely Manner

(U) Contracting officers did not review COR files to determine in a timely manner whether the CORs performed all duties in the designation letters. DFARS PGI subpart 201.6 requires contracting officers to review COR files once annually, and DoD Instruction 5000.72 requires the annual review to occur in the anniversary month of the COR's designation. At the time of our audit, the CORs for the ENCORE III task orders had been in place for less than a year, and therefore, the contracting officers were not yet required to review the COR files. Of the five task orders, only the contracting officer for the JSP Task Order elected to review the COR files early, in February 2020, which was 7 months before the September 2020 anniversary of the CORs' designation for this task order. At that time, the contracting officer determined that the CORs were not meeting the designation letter requirements and gave them time to meet those requirements. When the CORs did not meet the requirements, the contracting officer had sufficient support to replace the JSP CORs in September 2020.

(U) The contracting officer is ultimately responsible for the contract, and therefore, it is in the contracting officer's and the DoD's best interest to ensure that CORs are complying with all designation letter requirements. This is particularly relevant at the beginning of a contract to ensure that the COR is capable of performing all duties in the designation letter. As discussed in the "DoD Component CORs Did Not Properly Oversee Contractor Performance" section of this report, our results show that waiting a year to review COR files is insufficient oversight to detect and correct COR performance problems in a timely manner.

(U) The Principal Director of Defense Pricing and Contracting (DPC), Office of the Under Secretary of Defense for Acquisition and Sustainment, is responsible for the DoD-wide COR program and maintains the DFARS, the DFARS PGI, and DoD Instruction 5000.72. Therefore, the DPC Principal Director, Office of the Under Secretary of Defense for Acquisition and Sustainment, should direct the Defense Acquisition Regulations Council to revise DFARS PGI subpart 201.6 to require contracting officers to:

- (U) conduct an initial review of the COR file within a set timeframe, such as within 6 months, of designating a COR to ensure that the COR is complying with the designation letter requirements;

- (U) after the initial review, establish a COR file review frequency not less than once annually, based on the contracting officer's assessment of the risks, complexity, and value of the contract; and

- (U) provide comments to the COR and requiring activity within 30 days of a review on the COR's level of compliance with designation letter requirements and require the COR to take corrective action, as needed.[28]

(U) In addition, the DPC Principal Director, Office of the Under Secretary of Defense for Acquisition and Sustainment, should revise DoD Instruction 5000.72 to align with the updated COR file review requirements in DFARS PGI subpart 201.6. Furthermore, the DPC Principal Director, Office of the Under Secretary of Defense for Acquisition and Sustainment, should develop and issue interim guidance addressing initial and recurring COR file review requirements until DFARS PGI subpart 201.6 and DoD Instruction 5000.72 are revised and implemented.

(U) DoD COR Training Did Not Include Instruction on Interim Voucher Reviews

(U) DoD COR training did not include instruction on how to review interim vouchers. DoD Instruction 5000.72 requires that CORs complete Defense Acquisition University (DAU)-sponsored or equivalent COR training to prepare CORs for their responsibilities.[29] The Instruction states that a COR should complete a basic or advanced COR course, depending on the complexity and risk associated with the contract the COR will oversee.[30] The Instruction identifies that on completion of training, CORs should be able to perform their responsibilities.

[28] (U) DoD Instruction 5000.35, "Defense Acquisition Regulations (DAR) System," October 21, 2008 (Incorporating Change 2, August 31, 2018), states that the Defense Acquisition Regulations Council Director is the DoD point of contact for all proposed revisions to the FAR, DFARS, and DFARS PGI on behalf of the DPC Principal Director.

[29] (U) The DAU President, under the authority of the Under Secretary of Defense for Acquisition and Sustainment, is responsible for establishing and providing acquisition training for DoD personnel who perform acquisition-related duties. The DAU President develops, maintains, and provides the DoD COR training courses. DoD Instruction 5000.72 states that DoD Components and commercial training vendors may sponsor COR training that is equivalent to the DAU's COR training, as determined by an independent professional organization in accordance with DoD requirements.

[30] (U) DAU course CLC106, "COR with a Mission Focus," is an online course intended for CORs who are responsible for contracts with limited complexity and risks, and we refer to this course as the basic COR training course. DAU course CLC222, "COR Course," is an online course intended for CORs responsible for all other contracts. DAU course COR222, "COR Course," is an in-person training course that is equivalent to CLC222 but can be tailored to the requests of specific contracting officers and CORs. Because CLC222 and COR222 are equivalent courses, we refer to both the CLC222 and COR222 courses as the advanced COR training courses.

(U) In addition, DoD Instruction 5000.72 required CORs to complete training in the PIEE System. According to the PIEE System Program Manager, the training in the PIEE System included instruction on the administrative processing of contractor payment requests, such as interim vouchers, in the PIEE System but did not include instruction on how to review interim vouchers.

(U) Although all of the CORs completed the advanced COR training courses in preparation for their COR oversight responsibilities, the courses did not include detailed instruction on how to review interim vouchers. Specifically, the training courses did not include instructions, explanations, or activities on how to:

- (U) determine whether an interim voucher was accurate and contractor expenses were reasonable, allowable, and incurred for a contract;
- (U) detect problems such as unsupported travel costs; or
- (U) determine the number and extent of interim voucher reviews necessary to detect and prevent improper payments.

(U) According to DAU officials, the training courses provide basic, high-level information about the contract oversight process rather than detailed instruction on how to perform COR responsibilities like reviewing interim vouchers. The DAU officials stated that the DAU offers workshops and additional resources that include detailed information about COR responsibilities.[31] However, DAU workshops and other resources are not required to become or serve as a COR. DoD Instruction 5000.72 states that the advanced COR training courses should prepare CORs to validate contractor payment requests, including interim vouchers, but the courses did not. Therefore, the DAU President should revise the DoD COR training curriculum and materials, in coordination with the DPC Principal Director and the DCAA Director, to include detailed instructions for CORs to review and validate that contractor payment requests, including interim vouchers, are commensurate with performance to prevent improper payments.

(U) CORs Did Not Meet Technical Experience Requirements to Oversee Cybersecurity Services

(U) Six of the eight CORs for the ENCORE III task orders did not meet the technical experience requirements to oversee the contractor cybersecurity services required by the task orders. DoD Instruction 5000.72 requires that CORs possess relevant experience in the technical, professional, or administrative fields that correspond to the responsibilities designated to the COR for a specific contract. DoD Manual 8570.01 establishes the technical experience requirements for CORs who monitor contractor performance and accept deliverables for contracts that include cybersecurity services.[32]

[31] (U) DAU officials stated that the DAU provides informal training and additional resources for CORs during the DAU's weekly COR Office Hours and on the publicly available DoD COR Community of Practice and DoD Procurement Toolbox websites.

[32] (U) DoD Manual 8570.01, "Information Assurance Workforce Improvement Program," December 19, 2005 (Incorporating Change 4, November 10, 2015).

(U) Among other requirements, the Manual requires that CORs monitoring cybersecurity services obtain cybersecurity certifications that satisfy DoD Information Assurance Management Level II requirements, such as the Certified Information Systems Security Professional and Certified Chief Information Security Officer certifications.[33] However, of the eight CORs assigned to oversee the five task orders, only two CORs had certifications that met the Information Assurance Management Level II requirements as shown in Table 4.

(U) Table 4. CORs With Information Assurance Management Level II Cybersecurity Certifications

(U) Task Order	Number of CORs Who Met Cybersecurity Certification Requirements	Number of CORs Who Did Not Meet Cybersecurity Certification Requirements	Total CORs
ACC	1	1	**2**
CNIC	0	2*	**2**
JSP	0	2	**2**
PEO–T	0	1*	**1**
PFPA	1	0	**1**
Total	**2**	**6**	**8 (U)**

*(U) One of the two CNIC CORs and the PEO–T COR possessed CompTIA A+ and Security+ certifications, which are not Information Assurance Management Level II cybersecurity certifications.
(U) Source: The DoD OIG.

~~(CUI)~~ The six CORs without relevant cybersecurity experience were not able to determine whether the contractors complied with the requirements for their task orders. For example, one of the CORs acknowledged that they were not familiar with the JSP Task Order's cybersecurity requirements and had difficulty determining whether the contractor's performance met the requirements.[34] In contrast, the COR for the PFPA Task Order was a Certified Information Systems Security Professional, and the COR [redacted].[35] Based on the COR's input, the WHS contracting officer [redacted] decided to end the PFPA Task Order [redacted].

[33] (U) DoD Manual 8570.01 states that Information Assurance Management Level II personnel are responsible for the cybersecurity of an information system within a DoD networking environment. Information Assurance Management Level II personnel may perform a variety of security-related tasks, including to monitor contractor performance of contract requirements related to cybersecurity.

[34] (U) Only one of the two JSP CORs performed technical monitoring and oversight for the JSP Task Order.

[35] ~~(CUI)~~ [redacted]

(U) DoD Instruction 5000.72 requires a requiring activity to nominate a qualified official to be the COR and a contracting officer to verify that the COR nominee is qualified by education, training, and experience to be the COR for a contract. CNIC, JSP, and PEO–T officials did not nominate qualified personnel to be the CORs, and none of the contracting officers for the five ENCORE III task orders we reviewed verified that the COR nominees possessed technical experience to oversee contractor cybersecurity services before designating them to perform COR responsibilities.[36] Requiring activity officials provided a variety of reasons for not nominating qualified personnel, including a lack of a skilled workforce within their organization. The contracting officers stated that they were not aware that CORs needed to possess specific technical experience to oversee contractor performance for cybersecurity services. Therefore, the DISA and USTRANSCOM Heads of the Contracting Activity should direct the contracting officers for the CNIC and PEO–T Task Orders to verify that the CORs meet DoD technical experience requirements to monitor contractor cybersecurity services and accept cybersecurity deliverables, and if necessary, designate new CORs who meet those requirements.[37] In addition, the DPC Principal Director, Office of the Under Secretary of Defense for Acquisition and Sustainment, should develop and implement plans, in coordination with the Principal Deputy Chief Information Officer (CIO), Office of the DoD CIO, to ensure that contracting officers are aware of the DoD technical experience requirements for CORs who monitor contractor cybersecurity services or accept cybersecurity deliverables.

(U) DoD Instruction 5000.72 and the COR designation letters prohibit CORs from re-delegating, re-designating, or otherwise transferring their COR responsibilities to other officials. However, for three of the five ENCORE III task orders we reviewed, the CORs did not possess technical experience, so they improperly relied on others to conduct inspections, which violated DoD guidance. The CORs for the JSP Task Order relied on eight JSP cybersecurity officials to review contractor performance. Similarly, the CORs for the CNIC and PEO–T Task Orders relied on other officials to review contractor performance but did not quantify how many. For these three task orders, the CORs accepted the contractor services without directly overseeing the contractors' performance. Having a COR accept the contractor's work for payment without being directly involved in monitoring contractor performance increases the risk to the DoD of paying for services not received. Therefore, the DISA and USTRANSCOM Heads of the Contracting Activity should direct the contracting officers for the CNIC and PEO–T Task Orders to require the CORs to notify the contracting officers when additional support is needed to assist with the technical monitoring, oversight, or administration of the task

[36] (U) The DISA and WHS contracting officers for the ACC and PFPA Task Orders designated CORs who met the requirements only because the requiring activities nominated individuals who were qualified.

[37] (U) We did not make a recommendation to the DISA Head of the Contracting Activity for the JSP Task Order because the task order expired.

(U) orders and, when needed, designate additional officials as CORs, in accordance with DoD guidance.[38]

(U) The DoD Paid $24.2 Million Without Reasonable Assurance That Contractor Information Technology Services Met Task Order Requirements

(U) The lack of COR oversight for the five ENCORE III task orders resulted in DoD officials paying $24.2 million without reasonable assurance that contractor information technology services met task order requirements, including $167,335 of travel costs that may not have been reasonable, allowable, or supported by records. ACC, CNIC, JSP, PEO–T, and PFPA officials relied on the information technology services to support their missions. Improper contract oversight limited the detection of contractor performance problems and the contracting officers' ability to hold contractors accountable for noncompliance with contract requirements, which could have resulted in mission failure.

(U) Other Matters of Interest

(U) DFARS subpart 239.71 states that agencies must ensure that cybersecurity is provided for information technology services in accordance with current policies, procedures, and statutes.[39] The DFARS subpart contains a list of applicable policies and procedures that agencies must comply with, but the list includes DoD Directive 8500.1 and DoD Instruction 8500.2, which were both canceled and replaced by DoD Instruction 8500.01 in 2014.[40] Therefore, the DPC Principal Director, Office of the Under Secretary of Defense for Acquisition and Sustainment, should direct the Defense Acquisition Regulations Council to revise DFARS subpart 239.71 to reflect current DoD cybersecurity policies.

[38] (U) We did not make a recommendation to the DISA Head of the Contracting Activity for the JSP Task Order because the task order expired.

[39] (U) DFARS Part 239, "Acquisition of Information Technology," Subpart 239.71, "Security and Privacy for Computer Systems."

[40] (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, canceled and replaced DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002, and DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

(U) Management Comments on the Finding and Our Response

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity stated that this report mischaracterizes that DISA CORs improperly re-delegated, re-designated, or otherwise transferred COR responsibilities to other officials. The Head of the Contracting Activity stated that the DoD COR Guidebook allows other individuals who have designated surveillance responsibilities to monitor contract performance.

(U) Our Response

(U) We disagree that our characterization of the DISA CORs' actions as improper is incorrect. During the audit, we determined that the CORs for the JSP and CNIC Task Orders relied on other officials, who were not designated surveillance responsibilities by the contracting officer, to monitor contract performance and accept contractor services. Allowing non-designated officials to conduct those duties violates DoD Instruction 5000.72 and the COR designation letters, which state that the COR cannot appoint, delegate, or re-delegate COR duties to another official.

(U) U.S. Transportation Command Comments

(U) The USTRANSCOM Head of the Contracting Activity did not agree that all CORs who monitor contract performance and accept deliverables for contracts that include cybersecurity services require an Information Assurance Management Level II certification. The Head of the Contracting Activity also disagreed that CORs using expertise from other individuals to monitor contractor performance equates to re-delegation, re-designation, or transference of COR duties, and that doing so violates DoD Instruction 5000.72.

(U) Our Response

(U) DoD Manual 8570.01 requires that CORs directly monitoring cybersecurity services obtain certifications that satisfy DoD Information Assurance Management Level II requirements. The PEO–T Task Order required the contractor to perform cybersecurity services and the contracting officer designated the COR to oversee contractor performance of the PEO–T Task Order. Therefore, the COR should have had a DoD Information Assurance Management Level II certification.

(U) With regard to COR delegation of oversight, we disagree that allowing other individuals to monitor contractor performance is consistent with DoD Instruction 5000.72. The Instruction clearly states that CORs are prohibited from re-delegating, re-designating, or otherwise transferring their COR responsibilities to other

(U) officials. Allowing individuals who are not designated as CORs by the contracting officer to monitor contractor performance, whether those individuals have expertise in cybersecurity services or not, is equivalent to the re-delegation, re-designation, or transference of COR duties, and therefore, violates the Instruction.

(U) Recommendations, Management Comments, and Our Response

(U) Revised Recommendation

(U) As a result of management comments, we revised Recommendation 4.d to change the title of the DoD CIO official identified in the recommendation and throughout the report to the Principal Deputy CIO, Office of the DoD CIO.

(U) Recommendation 1

(U) We recommend that the Defense Information Systems Agency Head of the Contracting Activity:

a. **(U) Establish controls to ensure that the contracting officers for task orders HC1028-19-F-6100 and HC1028-19-F-6320 monitor whether the contracting officer's representatives are completing inspections and maintaining records of those inspections in the contracting officer's representative surveillance files in the Procurement Integrated Enterprise Environment System.**

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity agreed, stating that the contracting officer and the contract specialist have established a process with the CORs to submit, maintain, and review the COR files within the PIEE System.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation detailing the contracting officer's process for ensuring that the CORs are completing inspections and maintaining records of the inspections within the PIEE System.

b. **(U) Direct the contracting officer for task order HC1028-19-F-6320 to establish controls to verify that the contracting officer's representatives submit surveillance reports in the Procurement Integrated Enterprise Environment System in accordance with their designation letters.**

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity agreed, stating that the contracting officer and the contract specialist have established a process with the CORs to submit, maintain, and review the COR files within the PIEE System.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation showing that the contracting officer and contract specialist established a process to ensure that the COR submits surveillance reports in the PIEE System in accordance with the COR designation letter.

c. (U) Direct the contracting officers for task orders HC1028-19-F-6100, HC1028-19-F-6101, and HC1028-19-F-6320 to review the contractors' claimed travel costs of $159,987 and recover from the contractors any costs that were not reasonable, allowable, or supported.

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity agreed, stating that the contracting officers have already engaged with the CORs to ensure that the CORs are sufficiently reviewing travel cost vouchers. The Head of the Contracting Activity stated that the contractor for task order HC1028-19-F-6100 has refunded $797 in costs that were not reasonable, allowable, or supported.

(U) Our Response

(U) Although the Head of the Contracting Activity agreed with the recommendation, they did not provide a plan for reviewing and recovering the remaining claimed travel costs. Therefore, the recommendation is unresolved. We request that the Head of the Contracting Activity provide a response to the final report within 30 days explaining how they plan to review and recover, if appropriate, the remaining $159,190 in claimed travel costs.

d. (U) Direct the contracting officer for task order HC1028-19-F-6320 to verify that the contracting officer's representatives meet DoD technical experience requirements to monitor contractor cybersecurity services and accept cybersecurity deliverables, and if necessary, designate new contracting officer's representatives who meet those requirements.

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity agreed, stating that the contracting officer will verify whether the COR or those designated under DoD policy to surveil contractor performance meet the technical experience requirements.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation showing that the assigned CORs have met the technical experience requirements needed to surveil contracts that include cybersecurity services or designated new CORs who meet the requirements.

e. **(U) Direct the contracting officer for task order HC1028-19-F-6320 to require the contracting officer's representatives to notify the contracting officer when additional support is needed to assist with the technical monitoring, oversight, or administration of the task order, and when needed, designate additional officials as contracting officer's representatives, in accordance with DoD guidance.**

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity agreed, stating that the contracting officer discussed the role of technical monitoring and oversight with the COR, and that the COR understands the need to request assistance, if necessary.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation showing that the contracting officer directed the COR to notify the contracting officer when additional support is needed to assist with technical monitoring of the task order.

(U) Recommendation 2

(U) We recommend that the U.S. Transportation Command Head of the Contracting Activity:

a. **(U) Establish controls to ensure that the contracting officer for task order HTC711-20-F-D012 monitors whether the contracting officer's representative is completing inspections and maintaining records of those inspections in a contracting officer's representative surveillance file in the Procurement Integrated Enterprise Environment System.**

(U) U.S. Transportation Command Comments

(U) The USTRANSCOM Head of the Contracting Activity agreed, stating that as of May 2020, the COR submits a monthly email to the contracting officer that includes a surveillance report and verification that the report has been uploaded into the PIEE System.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation detailing the contracting officer's process for ensuring that the COR is completing inspections and maintaining records of the inspections within the PIEE System.

b. (U) Revise the U.S. Transportation Command contracting regulations to require contracting officers to establish in contracting officer's representative designation letters that contracting officer's representatives must submit surveillance reports more than once annually.

(U) U.S. Transportation Command Comments

(U) The USTRANSCOM Head of the Contracting Activity agreed, stating that USTRANSCOM will update USTRANSCOM Instruction 7500.02 to require contracting officers to establish in COR designation letters that CORs must submit surveillance reports more than once annually. The Head of the Contracting Activity plans to implement the recommendation by October 1, 2023.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides a copy of the updated Instruction and we verify that the Instruction requires contracting officers to establish in COR designation letters that CORs must submit surveillance reports more than once annually.

c. (U) Direct the contracting officer for task order HTC711-20-F-D012 to verify that the contracting officer's representative meets DoD technical experience requirements to monitor contractor cybersecurity services and accept cybersecurity deliverables, and if necessary, designate new contracting officer's representatives who meet those requirements.

(U) U.S. Transportation Command Comments

(U) The USTRANSCOM Head of the Contracting Activity partially agreed, stating that the contracting officer will determine whether COR nominees possess the appropriate education, training, and experience to be the COR. The Head of the Contracting Activity plans to implement the recommendation by July 2023.

(U) Our Response

(U) Although the Head of the Contracting Activity partially agreed, the proposed actions meet the intent of the recommendation. Therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation showing that the assigned CORs have met the technical experience requirements needed to surveil contracts that include cybersecurity services.

d. (U) Direct the contracting officer for task order HTC711-20-F-D012 to require the contracting officer's representative to notify the contracting officer when additional support is needed to assist with the technical monitoring, oversight, or administration of the task order, and when needed, designate additional officials as contracting officer's representatives, in accordance with DoD guidance.

(U) U.S. Transportation Command Comments

(U) The USTRANSCOM Head of the Contracting Activity partially agreed, stating that the contracting officer will advise the COR to notify the contracting officer when additional support is needed.

(U) Our Response

(U) Although the Head of the Contracting Activity partially agreed, the action proposed meets the intent of the recommendation. Therefore, the recommendation is resolved but open. We will close the recommendation once the Head of the Contracting Activity provides documentation showing that the contracting officer directed the COR to notify the contracting officer when additional support is needed to assist with technical monitoring of the task order.

(U) Recommendation 3

(U) We recommend that the Washington Headquarters Services Head of the Contracting Activity:

a. (U) Revise the Washington Headquarters Services contracting regulations to require contracting officers to establish in contracting officer's representative designation letters that contracting officer's

(U) representatives must submit surveillance reports more than once annually.

(U) Washington Headquarters Services Comments

(U) The WHS Head of the Contracting Activity agreed, stating that WHS updated its Enterprise COR Program policy on January 27, 2023. They added that the updated policy includes language that requires contracting officers to review and approve COR status reports, files, and documentation for completeness on a monthly basis. The Head of the Contracting Activity included a copy of the updated Enterprise COR Program policy with their comments.

(U) Our Response

(U) Although the Head of the Contracting Activity agreed with the recommendation and provided the updated policy, the updated policy does not address the specifics of the recommendation. Therefore, the recommendation is unresolved. The policy states that the contracting officer must include a statement in the COR designation letter that identifies how often CORs are required to complete status reports. However, the updated policy does not require CORs to submit surveillance reports more than once annually. We request that within 30 days the Head of the Contracting Activity provide additional comments in response to the final report, identifying a plan to require contracting officers to establish in COR designation letters that CORs must submit surveillance reports more than once annually.

b. (U) Direct the contracting officer for task order HQ0034-19-F-0486 to review the contractor's claimed travel costs of $7,348 and recover from the contractor any costs that were not reasonable, allowable, or supported.

(U) Washington Headquarters Services Comments

(U) The WHS Head of the Contracting Activity agreed, stating that WHS officials recovered travel costs in July 2020.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the specifics of the recommendation. We verified that WHS officials reviewed the contractor's claimed costs and recovered $7,322 in costs that were not reasonable, allowable, or supported. Therefore, the recommendation is closed, and no further comments are required.

(U) Recommendation 4

(U) We recommend that the Principal Director of Defense Pricing and Contracting, Office of the Under Secretary of Defense for Acquisition and Sustainment:

a. **(U) Direct the Defense Acquisition Regulations Council to revise Defense Federal Acquisition Regulation Supplement Procedures, Guidance, and Information Part 201, "Federal Acquisition Regulation System," Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities," to require contracting officers to:**

    1. **(U) Conduct an initial review of the contracting officer's representative file within a set timeframe, such as within 6 months, of designating a contracting officer's representative to ensure that the contracting officer's representative is complying with the designation letter requirements.**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director partially agreed, stating that DPC will consider revising the DFARS PGI in accordance with the recommendation.

(U) Our Response

(U) Although the Principal Director partially agreed, the comments did not address the specifics of the recommendation. Therefore, the recommendation is unresolved. We request that within 30 days the Principal Director provide a response to the final report explaining how the Principal Director plans to implement the COR file review in the DFARS PGI.

    2. **(U) After the initial review, establish a contracting officer's representative file review frequency not less than once annually, based on the contracting officer's assessment of the risks, complexity, and value of the contract.**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director agreed, stating that DFARS PGI 201.602 requires the contracting officer to conduct an annual COR file review.

(U) Our Response

(U) Although the Principal Director agreed, the comments did not address the specifics of the recommendation. Therefore, the recommendation is unresolved. Although the DFARS PGI 201.602 requires the contracting officer to conduct an annual COR file review, it does not contemplate the need for additional or more frequent reviews based

(U) on the risks, complexities, and values of contracts. We request that within 30 days the Principal Director provide additional comments in response to the final report, identifying a plan to revise the DFARS PGI to establish a COR file review frequency based on the contracting officer's assessment of the risks, complexity, and value of the contract.

3. **(U) Provide comments to the contracting officer's representative and requiring activity within 30 days of a review on the contracting officer's representative's level of compliance with designation letter requirements and require the contracting officer's representative to take corrective action, as needed.**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director agreed, stating that DPC implemented the recommendation.

(U) Our Response

(U) Although the Principal Director agreed with the recommendation, the comments do not address the specifics of the recommendation. Therefore, the recommendation is unresolved. DoD Instruction 5000.72 does not require that contracting officers provide comments to the COR and requiring activity within 30 days or require the CORs to take corrective action, as needed. Therefore, we request that within 30 days the Principal Director provide additional comments in response to the final report, identifying a plan to revise the DFARS PGI to require contracting officers to provide comments within 30 days and to require CORs to take corrective action, as needed.

b. **(U) Revise DoD Instruction 5000.72, "DoD Standard for Contracting Officer's Representative (COR) Certification," March 26, 2015 (Incorporating Change 2, November 6, 2020), to align with the updated contracting officer's representative file review requirements in Defense Federal Acquisition Regulation Supplement Procedures, Guidance, and Information Part 201, "Federal Acquisition Regulation System," Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities."**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director agreed, stating that if DPC revises the DFARS PGI, DPC will make appropriate changes to DoD Instruction 5000.72.

(U) Our Response

(U) Comments from the Principal Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close

(U) the recommendation once the Principal Director provides the revised Instruction and we verify that it aligns with the updated DFARS PGI.

c. **(U) Develop and issue interim guidance addressing initial and recurring contracting officer's representative file review requirements until Defense Federal Acquisition Regulation Supplement Procedures, Guidance, and Information Part 201, "Federal Acquisition Regulation System," Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities," and DoD Instruction 5000.72, "DoD Standard for Contracting Officer's Representative (COR) Certification," March 26, 2015 (Incorporating Change 2, November 6, 2020), are revised and implemented.**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director partially agreed, stating that DPC will issue a memorandum outlining COR oversight responsibilities for contracting officers.

(U) Our Response

(U) Although the Principal Director partially agreed, the proposed actions meet the intent of the recommendation. Therefore, the recommendation is resolved but open. We will close the recommendation once the Principal Director provides a copy of the memorandum and we verify that it includes the COR file review requirements.

d. **(U) Develop and implement plans, in coordination with the Principal Deputy Chief Information Officer, Office of the DoD Chief Information Officer, to ensure that contracting officers are aware of the DoD technical experience requirements for contracting officer's representatives who monitor contractor cybersecurity services or accept cybersecurity deliverables.**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director partially agreed, stating that DPC, in coordination with the DoD CIO, will issue a memorandum reminding the contracting community of the technical experience requirements and the necessity of CORs to meet the requirements.

(U) Our Response

(U) Although the Principal Director partially agreed, the proposed actions meet the intent of the recommendation. Therefore, the recommendation is resolved but open. We will close the recommendation once the Principal Director provides a copy of the memorandum and we verify that it informs contracting officers of the technical experience requirements for CORs who monitor contractor cybersecurity services or accept cybersecurity deliverables.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the Chief of Policy and Oversight for the DoD CIO agreed with the recommendation but requested that we revise the coordinating party to the Principal Deputy CIO, Office of the DoD CIO instead of the Principal Deputy CIO for Cybersecurity, Office of the DoD CIO.

e. **(U) Direct the Defense Acquisition Regulations Council to revise Defense Federal Acquisition Regulation Supplement Part 239, "Acquisition of Information Technology," Subpart 239.71, "Security and Privacy for Computer Systems," to reflect current DoD cybersecurity policies.**

(U) Defense Pricing and Contracting Comments

(U) The DPC Principal Director agreed, stating that DPC will amend the DFARS to reflect the updated references, as necessary.

(U) Our Response

(U) Comments from the Principal Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Principal Director provides a copy of the updated DFARS that reflects current DoD cybersecurity policies.

(U) Recommendation 5

(U) We recommend that the Defense Acquisition University President revise the DoD contracting officer's representative training curriculum and materials, in coordination with the Principal Director of Defense Pricing and Contracting and the Director of the Defense Contract Audit Agency, to include detailed instructions for contracting officer's representatives to review and validate that contractor payment requests, including interim vouchers, are commensurate with performance to prevent improper payments.

(U) Defense Acquisition University Comments

(U) The DAU Chief of Staff, responding for the DAU President, agreed, stating that the DAU will coordinate with the DPC Principal Director and the DCAA Director to update the DoD COR training curriculum and materials.

(U) Our Response

(U) Comments from the Chief of Staff addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Chief of Staff provides the updated COR training curriculum that includes detailed instructions for CORs to review and validate contractor payment requests.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from April 2020 through January 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We obtained a list of ENCORE III task orders from DISA contracting officials. The list represented the universe of ENCORE III information technology service task orders as of March 31, 2020.[41] We compared the list with records obtained from the PIEE System and the Federal Procurement Data System-Next Generation and concluded that DoD Components awarded 25 ENCORE III information technology service task orders as of March 31, 2020.[42] We selected a nonstatistical sample of 5 of the 25 task orders to review, valued at $279.8 million, based on the total dollar value of the task orders, the DoD Components performing contract administration, the contract types awarded, and the period of performance for the task orders. For two of the five task orders, the DoD OIG indirectly received services as a customer of the DoD Components.[43] We confirmed with relevant DoD OIG acquisition, information technology, and security officials that the DoD OIG did not have any conflicts, disputes, or other disagreements with the DoD Components for these two task orders that would cause a third party to question our objectivity.

(U) We interviewed officials from the DAU, the Defense Logistics Agency, the DPC, and the Office of the DoD CIO to clarify our understanding of DoD policies and training for COR responsibilities. We also interviewed officials and obtained and analyzed records such as inspection records, surveillance reports, and interim vouchers from the following organizations.

- (U) CNIC

[41] (U) Although the ENCORE III contract is intended to support activities within the DoD, other Federal agencies may issue ENCORE III task orders using procedures authorized by the "Economy Act" (31 U.S.C. § 1535 [1984]) and FAR Part 17, "Special Contracting Methods," Subpart 17.5, "Interagency Acquisitions."

[42] (U) The Federal Procurement Data System-Next Generation is a web-based tool for agency officials to report the award of contracts and task orders.

[43] (U) The JSP Task Order provided support to hundreds of information systems operated by the Office of the Secretary of Defense, the Joint Staff, and DoD agencies, including systems operated by the DoD OIG. The PFPA Task Order provided support to physical security systems that were critical to the security of DoD facilities at which the DoD OIG is a tenant.

- (U) DCAA
- (U) Defense Finance and Accounting Service
- (U) DISA
- (U) JSP
- (U) Joint Staff
- (U) PFPA
- (U) USTRANSCOM
- (U) WHS

(U) We reviewed COR designation records and qualification records to verify that requiring activities and contracting officers selected qualified personnel to perform oversight. We reviewed quality assurance surveillance plans to determine whether CORs developed plans to oversee contractor performance, and we also reviewed COR records from November 1, 2019, through April 30, 2020, to verify that the CORs performed oversight of contractor performance to ensure contractor services complied with task order requirements.

(U) On June 15, 2021, a DISA contracting officer awarded ENCORE III task order HC1028-21-F-6001 to provide information technology support to the DoD OIG's information systems. The contractor supporting this task order was the same contractor that supported the PFPA Task Order that we reviewed as part of the audit. We assessed the independence threats posed by the contractual relationships between the DoD OIG, the DISA contracting activity, and the contractor, and we applied safeguards that reduced the threats to an acceptable level.

(U) We provided an opportunity to the contractors for task orders HQ0034-19-F-0486, HC1028-19-F-6100, HC1028-19-F-6101, and HC1028-19-F-6320 to review and comment on relevant portions of the draft report. The contractors for task orders HQ0034-19-F-0486 and HC1028-19-F-6320 provided comments, while the contractors for task orders HC1028-19-F-6100 and HC1028-19-F-6101 elected not to provide comments. Any comments provided were considered in preparing the final report.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments

(U) submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed internal controls for designating CORs and the performance of COR oversight responsibilities. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We obtained a list of task orders from DISA contracting officials to determine the universe of ENCORE III task orders. We compared the list with contract documents from the PIEE System and the Federal Procurement Data System-Next Generation to confirm that the universe was complete. Although we determined that the list was inaccurate, we concluded that it was sufficiently reliable to determine the universe of task orders.

(U) Use of Technical Assistance

(U) We obtained assistance from the DoD OIG's Quantitative Methods Division for our nonstatistical sample of task orders. Quantitative Methods Division personnel reviewed and provided input for our sampling methodology.

(U) Prior Coverage

(U) No prior coverage has been conducted on contract oversight of information technology services at DISA, USTRANSCOM, or WHS during the last 5 years.

(U) Appendix B

(U) Contracting and Requiring Activities Reviewed

(U) Contracting officers and CORs at the following contracting activities and requiring activities administered the five ENCORE III task orders reviewed.

(U) Contracting Activities

(U) Defense Information Systems Agency

(U) DISA's Defense Information Technology Contracting Organization is a full-service contracting activity specializing in information technology, telecommunications, satellite bandwidth, combat support computing, and enterprise services, including enterprise licensing agreements, cloud services, mobility services, satellite phones, and desktop procurements supporting the DoD and various non-DoD organizations.

(U) U.S. Transportation Command

(U) USTRANSCOM's Directorate of Acquisition is the contracting activity responsible for the procurement of transportation and transportation-related services in support of USTRANSCOM's full-spectrum deployment and distribution mission to project and sustain the Joint Force around the world.

(U) Washington Headquarters Services

(U) The WHS's Acquisition Directorate is the contracting activity responsible for providing acquisition services to the Office of the Secretary of Defense, DoD agencies, and Federal agencies in the National Capital Region. WHS contracting officers support the procurement of a wide range of services for various U.S. Government-owned and leased facilities, including the Pentagon.

(U) Requiring Activities

(U) Commander, Navy Installations Command

(U) The CNIC is responsible for worldwide U.S. Navy shore installation management as the Navy's shore integrator. The CNIC Fleet and Family Readiness Directorate is responsible for policy development, implementation, and oversight of quality of life programs for Sailors and their families, including relocation assistance, new parent support, deployment services, clinical counseling services, financial management counseling, family employment services, family advocacy, and the transition assistance programs.

(U) Joint Service Provider

(U) The JSP, a DISA component, operates and defends the DoD's key cyber terrain and provides information technology services to Pentagon and National Capital Region customers. The JSP supports 55,000 customers and 70,000 assets, provides more than 80 information technology services to DoD headquarters organizations, and defends DoD networks against cyber attacks.

(U) Air Combat Command

(U) The ACC is responsible for organizing, training, and equipping combat-ready conventional and information warfare forces on behalf of the U.S. Air Force. The ACC's 318th Cyberspace Operations Group trains cyber operations personnel, develops cyber capabilities, operationally tests cyber systems, and maintains cyber range environments for U.S. Air Force, joint, and allied cyber training and exercises.

(U) Pentagon Force Protection Agency

~~(FOUO)~~ PFPA is responsible for force protection, security, and law enforcement for the Pentagon Reservation and DoD-occupied facilities in the National Capital Region. The PFPA Security Integration and Technology Directorate performs [redacted].

(U) U.S. Transportation Command

(U) USTRANSCOM is the unified, functional combatant command responsible for conducting global mobility operations and providing capabilities necessary to project and sustain the Joint Force in support of U.S. national objectives. The PEO–T, a subordinate organization within USTRANSCOM, provides oversight and management of acquisition programs for the development, fielding, and sustainment of USTRANSCOM capabilities. The PEO–T includes officials from USTRANSCOM's Directorate of Acquisition; Program Analysis and Financial Management Directorate; and Command, Control, and Cyber Systems Directorate.

(U) Appendix C

(U) Summary of the Notice of Concern, DISA Comments, Our Response, and DISA Actions Taken

(U) Notice of Concern Suggested Actions

(U) During the audit, we issued a notice of concern to the DISA Director that JSP officials were proposing modifications to revise the requirements for the JSP Task Order. We suggested that the DISA contracting officer consult with the DISA General Counsel, the DISA Competition Advocate, and other subject matter experts, as appropriate, to determine whether the JSP's proposed modifications were within the scope of the JSP Task Order. If the proposed modifications were out of scope, we suggested that the DISA contracting officer consider other courses of action, such as engaging in a competitive procurement to replace the JSP Task Order.

(U) DISA Director Comments

~~(CUI)~~ DISA's Assistant to the Director, responding for the DISA Director, stated that the DISA contracting officer would consult with the DISA General Counsel, DISA Competition Advocate, and other subject matter experts. The Assistant to the Director identified that [redacted].[44]

(U) Our Response

(U) Comments from the Assistant to the Director addressed our suggested actions, and the Director is not required to provide additional comments.

(U) DISA Actions Taken

~~(CUI)~~ On March 31, 2021, a DISA contracting officer modified the JSP Task Order. According to the DISA contracting officer, [redacted].

(U) Subsequently, on December 23, 2021, a DISA contracting officer awarded task order HC1028-22-F-0003 to replace the JSP Task Order and allowed the JSP Task Order to expire on February 24, 2022. The DISA contracting officer and JSP officials put $20.1 million to better use by allowing the JSP Task Order to expire and issuing task order HC1028-22-F-0003.

[44] ~~(CUI)~~ [redacted]

(U) Notice of Concern

~~CUI~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

September 14, 2020

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: (U) Potential Out-of-Scope Task Order Modification Identified During the Audit of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)

(U) This memorandum is being issued based on concerns identified during our audit of the Defense Information Systems Agency's (DISA) ENCORE III information technology services contract.[1] The objective of the audit is to determine whether DoD Components are administering task orders issued under the ENCORE III contract in accordance with Federal and DoD requirements. The work conducted on this audit is preliminary, and there is additional work ongoing to satisfy the audit objective. We are providing this memorandum for your comments and action before the completion of our audit.

(U) During the audit, we reviewed sole source task order HC1028-19-F-6101 administered by the Defense Information Technology Contracting Organization (DITCO) on behalf of the Joint Service Provider (JSP).[2] The task order performance work statement (PWS) requires the contractor to provide the JSP and its customers with cybersecurity services valued at $65.9 million, but does not clearly describe all the services to be performed as required by section 2304c, title 10, United States Code (10 U.S.C. § 2304c [2016]).[3] During interviews from June through August 2020, DITCO contracting officers acknowledged that the contractor's responsibilities were insufficiently detailed in the PWS, and a JSP acquisition management official stated that the task order was "not contractually viable."

~~(CUI)~~ To ensure that the contractor's responsibilities are adequately defined in the PWS, the JSP acquisition management officials submitted a modification package to the DITCO contracting officer on July 10, 2020.[4] The modification package includes a revised PWS and an independent government cost estimate for the services to be provided. We reviewed the

~~**Controlled by:** Audit / Cyberspace Operations~~
~~**CUI Category:** General Privacy, Source Selection~~
~~**Distribution / Dissemination Control:** Federal Employees Only~~
~~**POC:**~~ [redacted]

[1] (U) The ENCORE III contract is a multiple award, task order contract, and the DITCO contracting officer awarded the ENCORE III contract to 40 contractors.
[2] (U) DITCO is DISA's internal contracting activity.
[3] (U) Under the task order, the contractor provides IT services, solutions, and support to the Office of the Secretary of Defense, the Joint Staff, and other DoD organizations, including the DoD Office of Inspector General.
[4] (U) According to JSP records, JSP acquisition management officials were developing the modification as early as December 2019.

~~CUI~~

(U) Notice of Concern (cont'd)

~~CUI~~

~~(CUI)~~ modification package and are concerned that the modification will materially change the scope of the PWS. For example, the modification will [redacted] Furthermore, according to the independent government cost estimate, the modifications will increase the cost of services by [redacted], which will represent a [redacted] cost increase over the remaining duration of the task order.

(U) The U.S. Supreme Court has held that government officials cannot revise contracts at will and changes are "confined to what was fairly and reasonably within the contemplation of the parties when the contract was made."[5] In adjudicating protests to alleged out-of-scope modifications, the Comptroller General has identified that material changes in the type of work, performance period, or the costs between the contract as awarded and as modified demonstrate an out-of-scope modification.[6] Furthermore, the Comptroller General has held that out-of-scope modifications are subject to statutory competition requirements. Under section 2304, title 10, United States Code (10 U.S.C. § 2304 [2019]), DoD agencies "shall obtain full and open competition through the use of competitive procedures" for the procurement of services, with limited exceptions. If the DITCO contracting officer issues the JSP's proposed modifications, DISA may violate 10 U.S.C. § 2304 (2019) and expose itself to protests from contractors, including the other 39 ENCORE III contractors.

(U) Therefore, we suggest that the DITCO contracting officer consult with the DISA General Counsel, the DISA Competition Advocate, and other subject matter experts, as appropriate, to determine whether the proposed task order modifications are within the scope of task order HC1028-19-F-6101, and if out of scope, then consider other courses of action, such as engaging in a competitive procurement to replace task order HC1028-19-F-6101.

~~(CUI)~~ Please identify the actions you have taken as well as any planned or ongoing actions in response to this memorandum by October 2, 2020. This memorandum, your comments, and any actions taken will be included in our final report. If you have any questions, please contact [redacted].

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

[5] (U) *Freund v. United States*, 260 U.S. 60, 63 (1922).
[6] (U) Comptroller General Decision B-276659.2, "MCI Telecommunications Corporation," September 29, 1997.

2
~~CUI~~

(U) Management Comments

~~CUI~~

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL (DoDIG)

SUBJECT: (U) Potential Out-of-Scope Task Order Modification Identified During the Audit of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)

(U) Thank you for the opportunity to address DoDIG concerns provided in your 14 Sep 20 memorandum, subject as above, related to an in-process procurement action to support mission critical cyber defense work for the Defense Information Systems Agency (DISA) Joint Service Provider (JSP). In the course of the subject audit, the DoDIG noted concerns regarding contemplated changes to an ENCORE III Task Order (HC1028-18-D-0006, HC1028-19-F-6101) with Booz Allen Hamilton (BAH) for Cyber Security Consolidation (CSC) (hereinafter referred to as the Task Order).

~~(CUI)~~ Background on the Task Order is needed for the context of current actions. [redacted]

~~(CUI)~~ [redacted]

~~CUI~~

(U) Management Comments (cont'd)

~~CUI~~

DISA Memo, (U) Potential Out-of-Scope Task Order Modification Identified During the Audit of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)

[redacted]

~~(CUI)~~ Additionally, [redacted] as recommended in the DoDIG memorandum and consistent with existing Agency policy, the contracting officer will consult with DISA's General Counsel, Competition Advocate and other subject matter experts [redacted]

(U) My point of contact in this matter is the Head of Contracting Activity, [redacted]

YEE.GARRETT.SU[redacted]
NG.[redacted]

GARRET S. YEE
Major General, USA
Senior Procurement Executive

2

~~CUI~~

(U) Appendix D

(U) Summary of Potential Monetary Benefits

~~(CUI)~~ Table 5 identifies questioned costs, disallowed costs, and funds put to better use. DISA and WHS contracting officers could recover $167,335 from contractors because travel costs were not reasonable, allowable, or supported by records. In addition, DISA contracting officers put [redacted] to better use by not issuing a modification to the JSP Task Order, by allowing the task order to expire, and by issuing a replacement task order.

(U) Table 5. Potential Monetary Benefits

~~(CUI)~~ (U) Recommendation	(U) Type of Benefit	(U) Amount of Benefit	(U) Account
(U) 1.c	(U) Questioned costs	(U) 159,987	(U) Treasury Index 97X4930.005
(U) 3	(U) Disallowed costs	(U) 7,322	(U) Treasury Index 97X4931.000
	(U) Questioned costs	(U) 26	
(U) Notice of Concern Suggested Actions	(U) Funds put to better use	~~(CUI)~~ [redacted]	(U) Treasury Index 97X4930.005
	(U) Funds put to better use	(U) 20,106,825	
(U) Total Potential Monetary Benefits		~~(CUI)~~ [redacted]	~~(CUI)~~

(U) Source: The DoD OIG.

(U) Management Comments on the Potential Monetary Benefits and Our Response

(U) Defense Information Systems Agency Comments

(U) The DISA Head of the Contracting Activity stated that the potential monetary benefits associated with the Notice of Concern's suggested actions are the sum of the remaining option year value of the task order and the estimated value of a contemplated modification. The Head of the Contracting Activity also stated that the contractor for task order HC1028-19-F-6100 has already refunded $797 in questioned costs.

(U) Our Response

(U) Comments from the Head of the Contracting Activity partially addressed the potential monetary benefits. We request that the Head of the Contracting Activity provide additional comments on the remaining $159,190 in claimed travel costs.

(U) Washington Headquarters Services Comments

(U) The WHS Head of the Contracting Activity stated that the WHS Acquisition Directorate Enterprise Security Services Division took immediate action to recover $7,322 in disallowed travel costs.

(U) Our Response

(U) Comments from the Head of the Contracting Activity addressed the potential monetary benefits. No further comments are required.

(U) Management Comments

(U) Defense Contracting and Pricing Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT CYBERSPACE OPERATIONS, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to the Department of Defense Inspector General's Draft Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)

As requested, I am providing a response to recommendation 4 of the subject report.

Recommendation 4: The Department of Defense Inspector General (DoD IG) recommends the Principal Director, Defense Pricing and Contracting (DPC), Office of the Under Secretary of Defense for Acquisition and Sustainment:

a. Direct the Defense Acquisition Regulations Council to revise Defense Federal Acquisition Regulation Supplement Procedures, Guidance, and Information (DFARS PGI) Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities," to require contracting officers to:

1. Conduct an initial review of the contracting officer's representative file within a set timeframe, such as within 6 months, of designating a contracting officer's representative to ensure that the contracting officer's representative is complying with the designation letter requirements.

   Response: Partially concur; DPC will consider amending the DFARS PGI, in accordance with the recommendation.

2. After the initial review, establish a contracting officer's representative file review frequency not less than once annually, based on the contracting officer's assessment of the risks, complexity, and value of the contract.

   Response: Concur; action complete. DFARS PGI 201.602-2(d)(vii) requires the Contracting Officer to conduct an annual file review.

3. Provide comments to the contracting officer's representative and requiring activity within 30 days of a review on the contracting officer's representative's level of compliance with designation letter requirements and require the contracting officer's representative to take corrective action, as needed.

   Response: Concur; action complete. Consistent with current instruction, found at DoDI 5000.72 page 11.

b. Revise DoD Instruction (DoDI) 5000.72, "DoD Standard for Contracting Officer's Representative (COR) Certification," March 26, 2015 (Incorporating Change 2, November 6,

(U) Defense Pricing and Contracting Comments (cont'd)

2020), to align with the updated contracting officer's representative file review requirements in DFARS PGI Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities.

Response: Partially concur; Based on the outcome of recommendation 4.a.1., DPC will make appropriate changes to related instruction.

c. Develop and issue interim guidance addressing initial and recurring contracting officer's representative file review requirements until DFARS PGI Subpart 201.6, "Career Development, Contracting Authority, and Responsibilities," and DoDI 5000.72, "DoD Standard for Contracting Officer's Representative (COR) Certification," March 26, 2015 (Incorporating Change 2, November 6, 2020), are revised and implemented.

Response: Partially concur; DPC will issue a memorandum reminding contracting officers of their COR oversight responsibilities.

d. Develop and implement plans, in coordination with the Principal Deputy Chief Information Officer for Cybersecurity, Office of the DoD Chief Information Officer, to ensure that contracting officers are aware of the DoD technical experience requirements for contracting officer's representatives who monitor contractor cybersecurity services or accept cybersecurity deliverables.

Response: Partially concur; In coordination with CIO, DPC will issue a memorandum to remind the requirements and contracting communities of the necessity for CORs to have appropriate DoD technical experience requirements.

e. Direct the Defense Acquisition Regulations Council to revise DFARS Part 239, "Acquisition of Information Technology," Subpart 239.71, "Security and Privacy for Computer Systems," to reflect current DoD cybersecurity policies.

Response: Concur; DPC will follow the normal process for amending the DFARS, as necessary, to reflect updated references.

My point of contact for this matter is [redacted] in the office of Defense Pricing and Contracting, Contract Policy, who may be reached at [redacted].

Sincerely,

TENAGLIA.J[redacted]
OHN.M.[redacted]

John M. Tenaglia
Principal Director,
Defense Pricing and Contracting

(U) Defense Acquisition University Comments

DEPARTMENT OF DEFENSE
DEFENSE ACQUISITION UNIVERSITY
OFFICE OF THE PRESIDENT
9820 BELVOIR ROAD
FORT BELVOIR, VA 22060-5565

January 26, 2023

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT CYBERSPACE OPERATIONS, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to DoDIG Draft Report on (U) Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)

As requested, I am providing responses to the general content and recommendations contained in the subject report.

Recommendation 5:

We recommend that the Defense Acquisition University President revise the DoD contracting officer's representative training curriculum and materials, in coordination with the Principal Director of Defense Pricing and Contracting and the Director of the Defense Contract Audit Agency, to include detailed instructions for contracting officer's representatives to review and validate that contractor payment requests, including interim vouchers, are commensurate with performance to prevent improper payments.

Response:

Concur. DAU's COR 222V, Contracting Officer's Representative Course, is a virtual instructor-led training (VILT) course and is specifically designed for contracting officer's representatives (CORs) who are responsible for assuring that contractors perform in accordance with the terms and conditions of the contract. COR 222V provides CORs the breadth of knowledge required to perform their role, including: knowledge related to COR roles and responsibilities; basic contracting fundamentals; awareness of ethical and legal factors that impact COR responsibilities; and information necessary to make correct decisions to successfully execute COR responsibilities. CLC 222, Contracting Officer's Representative Online Training, is functionally the same course as COR 222V, but is delivered online. It provides the same course certification.

COR 222V and CLC 222 both provide high-level guidance for CORs to review and validate contractor payment requests. However, DAU concurs that these courses currently do not include detailed instructions for conducting interim voucher reviews.

Actions to be taken: DAU will coordinate with the Principal Director of Defense Pricing and Contracting and the Director of the Defense Contract Audit Agency in updating CLC 222 and COR 222V to address the concerns raised in the report.

Please contact [redacted], DAU's Center Director for Contracting & Small Business, [redacted] if additional information is required.

JOHNSON.JOSEPH.EDWIN. [redacted]

Joseph E. Johnson
Chief of Staff

(U) Defense Information Systems Agency Comments

~~CUI~~

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

23 January 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL (IG)

SUBJECT: Response to Draft Report for Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120)

Reference: DoDIG Draft Report: Audit of the Oversight of ENCORE III Information Technology Service Task Orders, dated 6 January 2022

On behalf of the Procurement Services Directorate (PSD), we appreciate the constructive dialogue with the DOD IG's office during the audit and on the scope of the draft findings. The results will be useful to PSD as we continually focus on improving our contract administration processes to provide superior contracting services to our mission partners across the Department.

~~(CUI)~~ DOD IG memorandum, dated 6 January, forwarding subject Draft Report. During the audit, we identified [redacted] in questioned costs, disallowed costs, and funds put to better use. The Defense Information Systems Agency and Washington Headquarters Services Directors must comment on these potential monetary benefits. If the Directors disagree with the potential monetary benefits, identify the amount and the reason for which you disagree.

~~(CUI)~~ Response: [redacted]

~~**Controlled by:** Procurement Services Directorate)~~
~~**CUI Category:** PROCURE~~
~~**Distribution/Dissemination Control:** FEDCON~~
~~**POC:**~~ [redacted]

~~CUI~~

(U) Defense Information Systems Agency Comments (cont'd)

~~CUI~~

SUBJECT: Response to Draft Report for Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120)

(U) Recommendations

(U) Recommendation 1.a. Establish controls to ensure that the contracting officers for task orders HC1028-19-F-6100 and HC1028-19-F-6320 monitor whether the contracting officer's representatives are completing inspections and maintaining records of those inspections in contracting officer's representative surveillance files in the Procurement Integrated Enterprise Environment System.

(U) Response: Concur. For both referenced task orders, the contracting officer (KO) has already coordinated with the contracting officer's representatives (COR) to ensure reporting within the Procurement Integrated Enterprise Environment (PIEE) system is current for performance through December 2022. Additionally, the KO and contract specialist have established a recurring coordination approach with the CORs for active submission, maintenance, and review of the COR files within PIEE. And finally, the task orders will be part of the population of contracts and orders considered for periodic inspection under the organization's review and self-inspection programs.

(U) Estimated Date of Completion: Complete

(U) Recommendation 1.b. Direct the contracting officer for task order HC1028-19-F-6320 to establish controls to verify that the contracting officer's representatives submit surveillance reports in the Procurement Integrated Enterprise Environment System in accordance with their designation letters.

(U) Response: Concur. As provided in the response to Recommendation 1.a., the KO has already coordinated with the COR to ensure reporting within PIEE is current for performance through December 2022. Additionally, the KO and contract specialist have established a recurring coordination approach with the CORs for active submission, maintenance, and review of the COR files within PIEE.

(U) Estimated Date of Completion: Complete

(U) Recommendation 1.c. Direct the contracting officers for task orders HC1028-19-F-6100, HC1028-19-F-6101, and HC1028-19-F-6320 to review the contractors' claimed travel costs of $159,987 and recover from the contractors any costs that were not reasonable, allowable, or supported.

(U) Response: Concur. The KOs have already engaged with the CORs to ensure cost

2

~~CUI~~

(U) Defense Information Systems Agency Comments (cont'd)

~~CUI~~

SUBJECT: Response to Draft Report for Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120)

vouchers for travel are (or were) sufficiently reviewed. Additionally, for the active orders (HC1028-19-F-6100 and HC1028-19-F-6320), the KO coordinated with the CORs to ensure future vouchers are subsequently reviewed as well. Based on recent reviews, the contractor for HC1028-19-F-6100 has refunded $797.25.

(U) Estimated Date of Completion: 28 February 2023

(U) Recommendation 1.d. Direct the contracting officers for task order HC1028-19-F-6320 to verify that the contracting officer's representatives meet DoD technical experience requirements to monitor contractor cybersecurity services and accept cybersecurity deliverables, and if necessary, designate new contracting officer's representatives who meet those requirements.

(U) Response: Concur, w/ caveat. The KO will verify if the COR or those designated under DoD policy to surveil contractor performance, and will ensure a qualified individual performs periodic review of deliverables for conformance with contract requirements. We find the report mischaracterizes that CORs may have improperly relied on other individuals to conduct inspections, which violated DoD guidance; and, purportedly re-delegated, re-designated, or otherwise transferred their COR responsibilities to other officials.

We appreciate the DOD IG highlighting the requirements of DOD Manual 8570.01. The requiring organization in good faith nominated a COR found to have the appropriate training, experience, and subject matter expertise for executing the CORs' duties. The KO verified the CORs met the training and certification requirements as outlined in the DoD COR Guidebook and DISA's COR Handbook prior to their designation. Further, the KO has discussed the surveillance role with the CORs to ensure a sufficient plan is in place for monitoring services and acceptance of deliverables. Considering the global nature of the task order and varying technical requirements, the KO understands that the CORs may need to coordinate with other Government officials prior to their acceptance of performance and deliverables.

This approach is consistent with Section 1.2 of the DoD COR Guidebook which states, "*Surveillance allows the government to verify the contractor is fulfilling contract delivery and quality requirements, and to document performance for the contract record. These individuals — (CORs) — function as the "eyes and ears" of the Contracting Officer and liaison between the government and contractor when executing specific technical and administrative functions and surveillance responsibilities (see FAR 2.101). However, these functions and contract*

3

~~CUI~~

(U) Defense Information Systems Agency Comments (cont'd)

~~CUI~~

SUBJECT: Response to Draft Report for Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120)

surveillance are not solely the responsibility of the Contracting Officer and the COR; other individuals may have designated surveillance responsibilities." (emphasis added).

Further, Section 3.4.5 states, "*Quality control personnel (e.g., quality assurance representative, quality assurance specialists, and quality assurance evaluators) may be assigned to assist with surveillance to ensure the contractor is in compliance with technical contractual requirements. They may be assigned as CORs or help the COR evaluate and document contractor performance, follow-up with the contractor on documented deficiencies, and provide input for performance evaluation reports.*"

(U) Estimated Date of Completion: 28 February 2023

(U) Recommendation 1.e. Direct the contracting officer for task order HC1028-19-F-6320 to require the contracting officer's representatives to notify the contracting officer when additional support is needed to assist with the technical monitoring, oversight, or administration of the task order, and when needed, designate additional officials as contracting officer's representatives, in accordance with DoD guidance.

(U) Response: Concur w/ caveat. The KO has discussed the role of technical monitoring and oversight with the COR, and the COR recognizes the need to request assistance if the required skills or certifications are not available to effectively surveil contract performance. As identified in the response to Recommendation 1.d., under DoD policy a COR may rely on quality control personnel to assist with surveillance.

(U) Estimated Date of Completion: 28 February 2023

The points of contact are [redacted] or [redacted], or the undersigned at [redacted].

PACKARD.DOUGL[redacted]
AS.W.[redacted]
DOUGLAS W. PACKARD
Procurement Services Executive
Director, Defense Information Technology
Contracting Organization

4

~~CUI~~

(U) U.S. Transportation Command Comments

UNITED STATES TRANSPORTATION COMMAND
508 SCOTT DRIVE
SCOTT AIR FORCE BASE, ILLINOIS 62225-5357

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: TCAQ

SUBJECT: DoD IG Draft Report "Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)"

1. The United States Transportation Command (USTRANSCOM) has reviewed the subject report and provides the attached response to the report's recommendations.

2. For additional information or assistance, please contact [redacted], TCIG, at [redacted].

BURTON.CHARLES.M.JR.[redacted]

CHARLES M. BURTON JR.
Head of the Contracting Activity

Attachment:
USTRANSCOM Response

cc:
TCIG
TCAQ
TCJA

(U) U.S. Transportation Command Comments (cont'd)

2

Corrective Action Plan (CAP)
Implementing Audit / External Assessment Recommendations

Subject: Draft Report for the Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000).

Recommendation 2: (U) We recommend that the USTRANSCOM Head of the Contracting Activity:

a. (U) Establish controls to ensure that the contracting officer for task order HTC711-20-F-D012 monitors whether the contracting officer's representative is completing inspections and maintaining records of those inspections in a contracting officer's representative surveillance file in the Procurement Integrated Enterprise Environment System.

(U) USTRANSCOM Position: *Concur. The Contracting Officer for task order HTC711-20-F-D012 monitors whether the contracting officer's representative is completing inspections and maintaining records of those inspections in a contracting officer's representative surveillance file in the Procurement Integrated Enterprise Environment System. As of May 2020, the contracting officer's representative submits a monthly email to the Contracting Officer that includes a monthly surveillance report as well as verification the report has been uploaded into the Procurement Integrated Enterprise Environment System.*

b. (U) Revise the U.S. Transportation Command contracting regulations to require contracting officers to establish in contracting officer's representative designation letters that contracting officer's representatives must submit surveillance reports more than once annually.

(U) USTRANSCOM Position: *Concur. The U.S. Transportation Command Acquisition Directorate, in coordination with the USTRANSCOM Command Directives Manager, will update USTCI 7500.02, Policy for The Contracting Officer's Representative Program. The update will require Contracting Officers to establish in Contracting Officer's Representative designation letters that Contracting Officers' Representatives must submit surveillance reports more than once annually. Estimated completion date is 01 October 2023.*

c. (U) Direct the contracting officer for task order HTC711-20-F-D012 to verify that the contracting officer's representative meets DoD technical experience requirements to monitor contractor cybersecurity services and accept cybersecurity deliverables, and if necessary, designate new contracting officer's representatives who meet those requirements.

(U) USTRANSCOM Position: *Partially concur. DoD Instruction 5000.72 requires a requiring activity to nominate a qualified official to be the Contracting Officer Representative (COR) and a Contracting Officer to determine the COR nominee possesses the appropriate education, training, and experience to be the COR. The COR will monitor all contractor cyber security services, accept cybersecurity deliverables, and ensure the contractor meets the cyber security requirements as specified in the contract. Estimated timeframe for the COR to meet the technical experience requirements is 3-6 months (July 2023). USTC does not agree all CORs who monitor contract performance and accept deliverables for contracts that include cybersecurity services require an IAM Level II certification specifically and requests revision of this paragraph.*

(U) U.S. Transportation Command Comments (cont'd)

d. (U) Direct the contracting officer for task order HTC711-20-F-D012 to require the contracting officer's representative to notify the contracting officer when additional support is needed to assist with the technical monitoring, oversight, or administration of the task order, and when needed, designate additional officials as contracting officer's representatives, in accordance with DoD guidance.

(U) USTRANSCOM Position: *Partially concur. The Contracting Officer for task order HTC711-20-F-D012 will advise the contracting officer's representative to notify the contracting officer when additional support is needed to assist with the technical monitoring, oversight, or administration of the task order, and when needed, in conjunction with the Requiring Activity, designate additional officials as contracting officer's representatives, in accordance with DOD guidance. Estimated completion date is February 2023. USTC does not agree CORs utilizing other expertise to accomplish COR duties equates to a re-delegation, re-designation, or transference of COR duties, nor is doing so in violation of DOD Instruction 5000.72, and requests revision of this paragraph.*

Additional Comments: *N/A*

CAP OPRs:

[redacted]
Contracting Officer
[redacted]

[redacted]
Procurement Analyst
[redacted]

CAP OCRs:

[redacted]
Procurement Analyst
[redacted]

(U) Washington Headquarters Services Comments

ACQUISITION DIRECTORATE

DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

January 31, 2023

[redacted]
Cyberspace Operations
US Department of Defense, Office of Inspector Genera
4800 Mark Center Drive
Alexandria, VA 22350-1500

Dear [redacted]

Washington Headquarters Services, Acquisition Directorate (WHS/AD) is in receipt of the Department of Defense Office of Inspector General's (DoD OIG's) Draft Report No. Project No. DODIG-2020-D000CT-0120.000 entitled "Audit of the ENCORE III Information Technology Service Task Orders, dated January 6, 2023. WHS/AD appreciates the opportunity to address and recommend closeout on the requested recommendations identified under 3.a and 3.b. in the referenced report.

Recommendations	WHS/AD Deliverables	Status
3.a. (U) Revise the Washington Headquarters Services contracting regulations to require contracting officer's representatives to submit surveillance reports more than once annually.	WHS AD finalized the Enterprise Contracting Officer Representative Program Updated policy in the Acquisition Directorate Acquisition Procedures PGI January 27, 2023 that includes language for monthly status reporting, which requires Contracting Officers to review and approve COR status report and files documentation for completeness on a monthly basis (unless other terms are authorized by AD policy).	Concur: Completed supporting documentation (attached).
3.b. (U) Direct the contracting officer for task order HQ0034-19-F-0486 to review the contractor's claimed travel costs of $7,348 and recover from the contractor any costs that were not reasonable, allowable, or supported.	WHS AD Enterprise Security Services Division upon discovery and analysis took immediate action to recover travel cost July 2020.	Concur: Completed.

Thank you for the opportunity to respond to the draft report recommendations, WHS/AD is committed to complying with all statutes, regulations and strengthening its internal controls to ensure full compliance with the OIG's recommendations. In addition, we are requesting the attached comments be considered for the final report. The assigned point of contact for this topic is [redacted] Division Director, Enterprise Acquisition Policy and Strategic Initiative. [redacted] can be reached at [redacted]

(U) Washington Headquarters Services Comments (cont'd)

Thank you for providing WHS/AD the opportunity to provide artifacts to support the closure for the draft report.

Respectfully,

SANDERS.DAVID.DE
LANO.[redacted]
David D. Sanders
Director

Attachments:

1. Procnote 2023-0003_ Update ADAP PGI Subpart 201.604-90, Enterprise Contracting Officer's Representatives (COR) Program Guidance

(U) Washington Headquarters Services Comments (cont'd)

DEPARTMENT OF DEFENSE

WASHINGTON HEADQUARTERS SERVICES

1155 DEFENSE PENTAGON

ACQUISITION DIRECTORATE

PROCUREMENT NOTICE

PROCNOTE 2023-0003
January 27, 2023

SUBJECT: Washington Headquarters Services (WHS) Acquisition Directorate (AD) Enterprise Contracting Officer Representative (COR) Program

REFERENCES.

(a) DoD Instructions 5000.72, "Standard for Contracting Officer's Representative (COR) Certification," 26 March 2015, updated Change 2, 06 November 2020
(b) FAR 1.602-2, "Responsibilities"
(c) DFARS Part 201.602-2
(d) DFARS PGI 201.602-2 Responsibilities
(e) Acquisition Directorate Acquisition Policy (ADAP) Subparts 201.604-90
(f) Procurement Integrated Enterprise Environment Web-Based Training

PURPOSE. This notice will establish the Washington Headquarters Services (WHS) Acquisition Directorate (AD) Enterprise Contracting Officers Representative (COR) Program. The program will include but not limited to structure, guidance, and COR incentive awards and recognitions.

POLICY. This policy shall be utilized for all WHS AD customers with contract actions requiring official COR designation and oversight for the period of performance of the contract awarded. The applicable guidance will be incorporated in ADAP Subpart 201.604-90, Enterprise Contracting Officer's Representatives (COR) Program, and ADAP PGI Subpart 201.604-90, Enterprise Contracting Officer's Representatives (COR) Program Guidance.

EFFECTIVE PERIOD. This PROCNOTE Update is effective immediately upon issuance.

[redacted]
EAPSI Director

(U) Washington Headquarters Services Comments (cont'd)

PROCNOTE 2023-0002

(a) Roles and Responsibilities

(1) EAPSI Division Director will:

(i) Provide management oversight of the COR Program
(ii) Work with AD leadership to ensure the program is implemented
(iii) Align and work with internal leads of WAWF/CPARS and other points of interest
(iv) Provide oversight of the COR incentive and recognition program
(v) Encourage innovation and streamline opportunities
(vi) Communicate with external components to enhance the program
(vii) Leverage Acquisition Workforce Community of Practice (AWCoP) to create an opportunity for COR participation
(viii) Align necessary resources to ensure the program is executed properly

(2) Lead COR Program Manager will:

(i) Provide oversight of the COR PIEE registration process and nomination/appointment process
(ii) Review and standardize specific COR designation letter data elements and COR reporting smart forms to be utilized within the Surveillance and Performance Monitoring (SPM) module
(iii) Work in conjunction with AD operations on training needs and trends to improve customer skills and ability, and enhance the customer experience
(iv) Advising AD leadership of issues, trends, best practices, and recommendations to improve CORs performance and documentation compliance across the serviced population
(v) Assist COs/CSs on COR-related issues within JAM and SPM
(vi) Collaborate and coordinate with e-Business on WAWF/Invoice/Acceptance Training
(vii) Collaborate and coordinate with CPARS focal point on training for CORs
(viii) Maintain a list of active CORs located in SPM
(ix) Review Active COR files documentation for-impending annual CORs file reviews
(x) Conduct annual guided discussions/forums (purpose: exchanges based on existing goals, successes, and breakdowns)
    1. COs/CSs
    2. CORs
(xi) Conduct annual structured update meetings as needed (purpose: open channel of communication for disseminating what is happening and policy/procedural changes)
    1. COs/CSs
    2. CORs
(xii) Offer assistance to CO and delegated CORs:
    1. Resources available through the WHS COR portal
    2. JAM and SPM training opportunities

2

(U) Washington Headquarters Services Comments (cont'd)

PROCNOTE 2023-0002

3. WHS AD COR training opportunities

(xii) Provide Division Directors and Branch Chief:

1. Current Awards Report (requires a COR Designation or COR Exemption MFR)
2. Active CORs with departing CO/CS SPM Report (This requires a CO/CS change)
3. Duplicate COR appointments in SPM Report (This requires updating COR type, termination, or canceling of duplicate action)
4. Inactive CORs Report

(b) Operational Division

(1) Contracting Officer

(i) Pre-Award

1. Register in PIEE for the CO role in SPM
2. Nominate and Appoint COR (Primary and Alternate) in JAM
   - Initiate the Primary COR nomination by either the COR self-nomination process or the Contracting Officer/Contract Specialist appointment utilizing in the Joint Appointment Module
   - Track the COR nomination process through either approving, rejecting, or canceling in the Joint Appointment Module
   - Ensure the Primary COR nomination is executed at the earliest opportunity
   - Initiate the Alternate COR nomination (recommended, not mandatory) in the same manner as the Primary COR

(ii) Post-Award

1. Ensure the Primary COR designation letter has been executed and viewable in SPM within 3-days of award or available for JAM retrieval from PIEE, Electronic Data Access (EDA) system
2. Must include the following statement(s) on the designation letter, section 14, Additional Duties:
   a. Must complete status reports within the SPM module (statement must state how often- i.e. monthly, quarterly, or as determined by contract terms, QASP, or applicable authority)
3. Must provide COR with:
   a. COR status report form to be utilized (SPM smart form or agreed upon form)
   b. Where to locate the COR status report form
   c. Instruction on how to complete the form, and
   d. How to upload COR Status Report form and supporting documentation to the COR File located in SPM
4. Review and approve COR status report and files documentation for completeness on a monthly basis (unless other terms are authorized by AD policy)

3

(U) Washington Headquarters Services Comments (cont'd)

PROCNOTE 2023-0002

5. Review, annually, the COR's files for accuracy and completeness.
    a. The date of the review should be on the anniversary of the COR's appointment
    b. The results of the contracting officer's review shall be conducted within and documented on the Annual COR File Inspection Checklist smart form located in SPM Module
6. Transfer active COR file in SPM with departing CO/CS with new CO/CS
    a. Required prior to departure of CO/CS
7. Invoice Payment Oversight
8. CO must ensure invoices are certified in WAWF in a timely manner by COR on a monthly basis; or retain invoices payment process
9. Quality Assurance Surveillance Monthly Monitoring
10. Contractor Performance Monthly Monitoring and Oversight
11. Government Furnished Property (GFP) joint annual review with the COR
12. Notify COR of impending annual CORs file reviews
13. Notify COR of refresher training 30 calendar days in advance of the due date

(2) Contracting Specialist will:
- (i) Register in SPM for the CS role
- (ii) Assist with nominating COR in JAM
- (iii) Work with CO to perform contract surveillance, oversight, and performance monitoring
- (iv) Conduct a COR contract file document review on a monthly basis
- (v) Communicate with the Contracting Officer Representative

(c) Enterprise Management Operation Division (EMOD) (eBusiness) provides oversight:

(1) Contractor Performance Assessment Reporting System (CPARS) Focal Point Lead
- (i) Register contracts/orders that will require a contractor performance evaluation
- (ii) Authorize CPARS and FAPIIS Access for COs, CSs, and CORs
- (iii) Provide COs, CSs, and CORs day-to-day assistance with CPARS and FAPIIS automated workflows
- (iv) Collect, distribute, and control evaluations and FAPIIS records
- (v) Continuously monitors the completion of assessments
- (vi) Identify non-compliant CPARs records and take necessary actions to make records compliant
- (vii) Collect CPARs metrics and report on a monthly basis
- (viii) Provide COs, CSs, and CORs training
- (ix) Ensure all WHS CPARs issues or concerns are resolved
- (x) Collaborate and coordinate with COR Program Team Lead on any updates on training requirements that may benefit the COR Community.

4

(U) Washington Headquarters Services Comments (cont'd)

PROCNOTE 2023-0002

(2) WAWF Invoice/Payment Lead

(i) Provide and assist COs, CSs, and CORs with PIEE and WAWF access

(ii) Provide COs, CSs, and CORs assistance with automated workflows

(iii) Provide COs, CSs, and CORs training

(iv) Send out Weekly List of Outstanding Submitted Invoices to COs, CSs, and CORs

(v) Troubleshoot/Research/Assist COs, CSs, and CORs with Invoicing and Payment Issues

(vi) Collaborate and coordinate with COR Program Team Lead on any updates on training

5

(U) DoD Chief Information Officer Comments

Final Report Reference

CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

January 26, 2023

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment on DoD Inspector General Draft Report "Audit of the Oversight of ENCORE III Information Technology Service Task Orders" (Project No. D2020-D000CT-0120.000)

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Report, Audit of the Oversight of ENCORE III Information Technology Service Task Orders (Project No. D2020-D000CT-0120.000)

DoD IG RECOMMENDATION: Among other recommendations, we recommend that the Principal Director of Defense Pricing and Contracting, Office of the Under Secretary of Defense for Acquisition and Sustainment:

- develop and implement plans, in coordination with the Principal Deputy Chief Information Officer for Cybersecurity, Office of the DoD Chief Information Officer, to ensure that contracting officers are aware of the DoD technical experience requirements for CORs who monitor contractor cybersecurity

Revised Recommendation 4.d

DoD CIO RESPONSE: DoD CIO agrees with the DoD IG recommendation and recommends the following correction/edit. Change the title of the DoD CIO official identified in the recommendations and throughout the report from "Principal Deputy Chief Information Officer for Cybersecurity, Office of the DoD Chief Information Officer" to "Principal Deputy Chief Information Officer (PDCIO), Office of the DoD Chief Information Officer" as the recommendation spans the work and portfolio areas of more than one Deputy Chief Information Officer over which the PDCIO exercises direction and authority.

A security review to verify "Controlled Unclassified Information" (CUI) markings in the report has been completed and there are no additional recommendations.

The point of contact for this matter is [redacted]. He can be reached at [redacted].

WOLFKILL.TIMOTHY[redacted]
.JAMES.[redacted]

Timothy J. Wolfkill
CSI Chief of Policy and Oversight
(DoD CIO GAO/IG Audits Liaison)

(U) Acronyms and Abbreviations

(U)	**ACC**	Air Combat Command
	CIO	Chief Information Officer
	CNIC	Commander, Navy Installations Command
	COR	Contracting Officer's Representative
	DAU	Defense Acquisition University
	DCAA	Defense Contract Audit Agency
	DFARS	Defense Federal Acquisition Regulation Supplement
	DISA	Defense Information Systems Agency
	DPC	Defense Pricing and Contracting
	FAR	Federal Acquisition Regulation
	JSP	Joint Service Provider
	PEO–T	Program Executive Office U.S. Transportation Command
	PFPA	Pentagon Force Protection Agency
	PGI	Procedures, Guidance, and Information
	PIEE	Procurement Integrated Enterprise Environment
	USTRANSCOM	U.S. Transportation Command
	WHS	Washington Headquarters Services (U)

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098