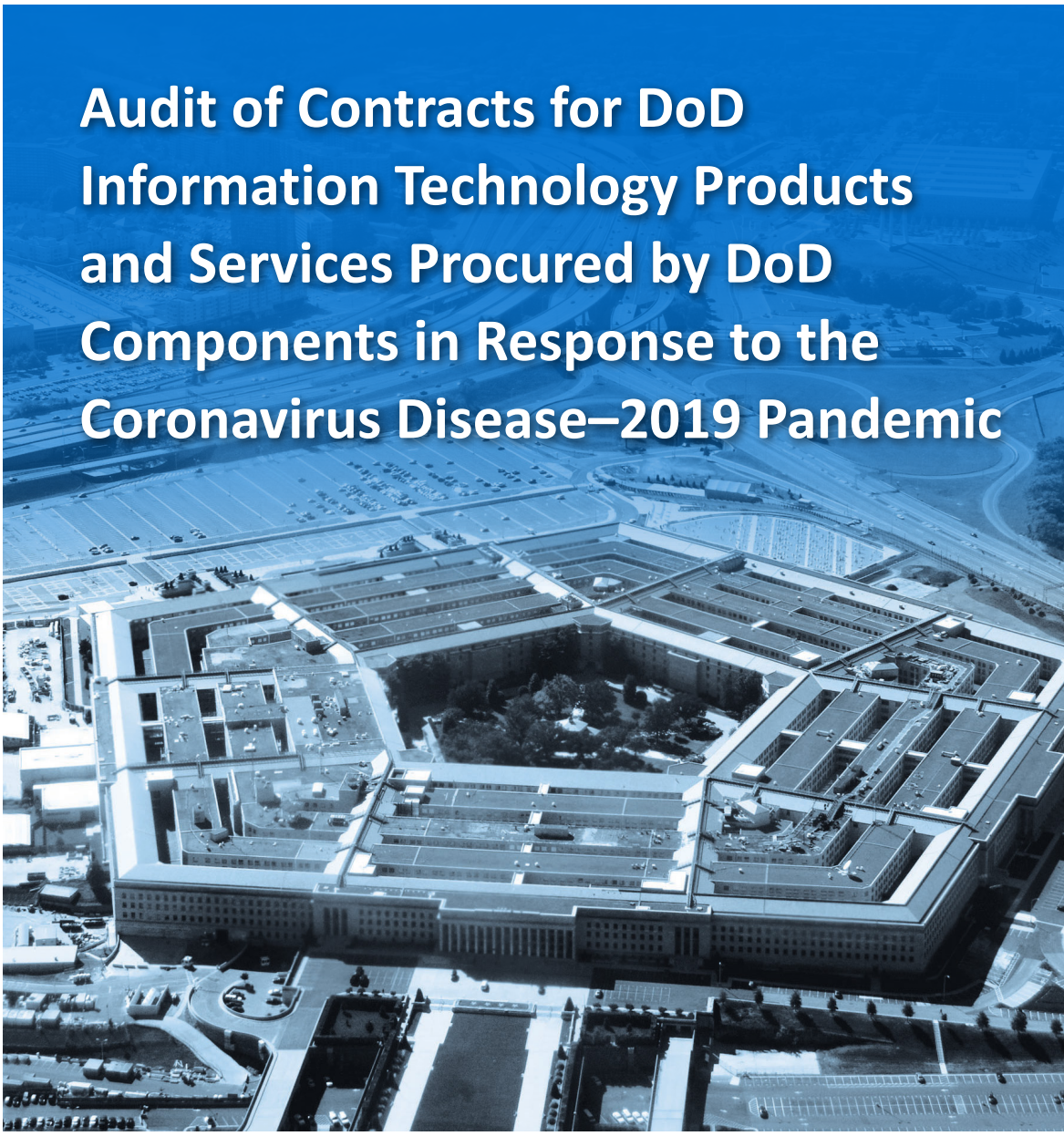
Report No. DODIG-2021-050

INSPECTOR GENERAL

U.S. Department of Defense

FEBRUARY 12, 2021

Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic

February 12, 2021

Objective

The objective of this audit was to determine whether DoD Components, in accordance with Public Law 116-136, "Coronavirus Aid, Relief, and Economic Security Act" (CARES Act) and other Federal and DoD requirements:

- procured information technology products and services to support operations in response to the coronavirus disease–2019 (COVID-19) pandemic;[1]
- paid fair and reasonable prices for those products and services;
- assessed whether known cybersecurity risks existed and developed risk mitigation strategies for the risks before procuring or using the information technology products; and
- accurately reported the required COVID-19-related codes to USAspending.gov.[2]

Background

COVID-19 is an infectious disease caused by a newly discovered coronavirus. On January 31, 2020, the Secretary of Health and Human Services declared a public health emergency due to confirmed cases of COVID-19 in the United States. On March 11, 2020, the World Health Organization declared the COVID-19 outbreak a pandemic, and on March 13, 2020, the President declared

[1] A pandemic is a global outbreak of a disease that occurs when a new virus emerges to infect people and can spread between people sustainably.

[2] USAspending.gov is a public website that policy makers and taxpayers can access to track U.S. Government spending and contract and grant data.

Background (cont'd)

the COVID-19 pandemic a national emergency as COVID-19 continued to spread across the country. On March 15, 2020, to protect the health and safety of the workforce, the Acting Director of the Office of Management and Budget issued a memorandum asking all Federal Executive Branch departments and agencies to offer maximum telework flexibilities to all eligible personnel. Two days later, on March 17, 2020, the Office of Management and Budget issued a memorandum directing agencies to begin implementing policies and procedures to safeguard the health and safety of Federal workplaces, including maximizing telework across the Nation for the Federal workforce, while ensuring that Government operations continue.

On March 27, 2020, the President signed the CARES Act, appropriating $2.2 trillion in additional funding for Federal agencies to prevent, prepare for, and respond to COVID-19, including $10.5 billion to the DoD. The CARES Act requires each Federal agency to develop a plan describing how it will spend CARES Act funds and to submit the plan to the Council of the Inspectors General on Integrity and Efficiency, Pandemic Response Accountability Committee. On May 29, 2020, the DoD submitted its CARES Act Spend Plan to the Committee, detailing how the $10.5 billion in CARES Act funds would be spent. The spend plan identified $323.6 million to procure information technology products and services to enhance the DoD's network capabilities, enforce social distancing, and support continuing operations within the maximum telework environment.

Finding

The Army, Navy, Air Force, Defense Health Agency, and Defense Information Systems Agency procured information technology products and services in accordance with the CARES Act and other Federal and DoD requirements. Specifically, for 28 of 367 nonstatistically sampled contract actions reviewed, the DoD Components:

- procured information technology products and services to support operations in response to the COVID-19 pandemic and provided contract documentation that supported that the contracts were issued to support the DoD's response to the pandemic;

Results in Brief

Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic

Finding (cont'd)

- paid fair and reasonable prices for products and services procured because their contracting officials completed and documented one or more Federal Acquisition Regulation-compliant price analysis techniques in their fair and reasonable price determinations;
- assessed whether known cybersecurity risks existed by running vulnerability scans before procuring or using the information technology products and developing corrective action plans for the vulnerabilities that could not be immediately mitigated; and
- accurately reported the COVID-19-related codes to USAspending.gov in accordance with Federal requirements. Army, Navy, Air Force, Defense Health Agency, and Defense Information Systems Agency contracting officials accurately reported the National Interest Action Code in the DoD FY 2020 second and third quarter Digital Accountability and Transparency Act submissions.

As a result of the DoD's compliance with the CARES Act and other Federal and DoD requirements, DoD stakeholders have assurance that the Army, Navy, Air Force, Defense Health Agency, and Defense Information Systems Agency procured $81.5 million in information technology products and services in response to the COVID-19 pandemic at reasonable prices and at a reduced risk of cybersecurity vulnerabilities. Continued DoD efforts to comply with the CARES Act and other Federal and DoD requirements will reduce the risk of waste, fraud, and abuse associated with the procurement of information technology products and services and ensure that the American public has visibility of DoD spending on contract actions associated with the response to COVID-19. Furthermore, continued DoD efforts to identify and mitigate cybersecurity vulnerabilities before procuring or using the information technology products and services, will reduce the risk of introducing vulnerabilities into DoD systems and networks that could potentially jeopardize the DoD's missions, information, and assets.

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

February 12, 2021

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DOD
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic (Report No. DODIG-2021-050)

This final report provides the results of the DoD Office of Inspector General's audit. We considered management comments on a discussion draft of this report when preparing this final report. We did not make any recommendations; therefore, no management comments are required.

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

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents

Introduction

Objective

The objective of this audit was to determine whether DoD Components, in accordance with Public Law 116-136, "Coronavirus Aid, Relief, and Economic Security Act" (CARES Act) and other Federal and DoD requirements:

- procured information technology products and services to support operations in response to the coronavirus disease–2019 (COVID-19) pandemic;[3]
- paid fair and reasonable prices for those products and services;
- assessed whether known cybersecurity risks existed and developed risk mitigation strategies for the risks before procuring or using the information technology products; and
- accurately reported the required COVID-19-related codes to USAspending.gov.[4]

See Appendix A for a discussion on the scope and methodology, and prior audit coverage related to our audit objective.

Background

COVID-19 is an infectious disease caused by a newly discovered coronavirus. On January 31, 2020, the Secretary of Health and Human Services declared a public health emergency due to confirmed cases of COVID-19 in the United States. On March 11, 2020, the World Health Organization declared the COVID-19 outbreak a pandemic, and on March 13, 2020, the President declared the COVID-19 pandemic a national emergency as COVID-19 continued to spread across the country. On March 15, 2020, to protect the health and safety of the workforce, the Acting Director of the Office of Management and Budget (OMB) issued a memorandum asking all Federal Executive Branch departments and agencies to offer maximum telework flexibilities to all eligible personnel. Two days later, on March 17, 2020, the OMB issued a memorandum directing agencies to begin implementing policies and procedures to safeguard the health and safety of Federal workplaces, including maximizing telework across the Nation for the Federal workforce, while ensuring that Government operations continue.[5] On March 27, 2020, the President signed the CARES Act, appropriating $2.2 trillion in additional funding for Federal agencies to prevent, prepare for, and respond to COVID-19, domestically and internationally,

[3] A pandemic is a global outbreak of a disease that occurs when a new virus emerges to infect people and can spread between people sustainably.

[4] USAspending.gov is a public website that policy makers and taxpayers can access to track U.S. Government spending and contract and grant data.

[5] OMB Memorandum M-20-16, "Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19," March 17, 2020.

including $10.5 billion to the DoD. The CARES Act requires each Federal agency to develop a plan describing how it will spend the CARES Act funds and to submit the plan to the Council of the Inspectors General on Integrity and Efficiency, Pandemic Response Accountability Committee (PRAC).[6] On May 29, 2020, the DoD submitted its CARES Act Spend Plan to the PRAC, detailing the plan to spend the $10.5 billion in CARES Act funds. The DoD CARES Act Spend Plan identified $323.6 million to procure information technology products and services to enhance the DoD's network capabilities, enforce social distancing, and support continuing operations within the maximum telework environment.

The information technology products and services that the DoD procured with the CARES Act funds included:

- hardware such as laptops, cell phones, and tablets;
- software such as virtual private networks and software licenses; and
- services such as information technology support.

Fair and Reasonable Prices

The Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) require contracting officers to procure supplies and services from responsible sources at fair and reasonable prices. The FAR requires contracting officers to determine whether a proposed price is fair and reasonable before awarding the contract. Fair and reasonable pricing may be determined by using price analysis, the process of examining and evaluating a proposed price without evaluating its separate cost elements and proposed profit. The FAR provides multiple price analysis techniques that contracting officers can use singly or in combination to determine price reasonableness.[7] These techniques include:

- comparing competitive quotes or offers (preferred method);
- comparing prices to historical prices from previous purchases;
- estimating methods to identify inconsistencies in price;
- comparing prices to current price lists, catalogs, or advertisements;
- comparing prices to an independent Government cost estimate (IGCE);
- comparing prices to those identified through market research for the same or similar items; or
- conducting analysis using certified or uncertified cost data.[8]

[6] The Council of the Inspectors General on Integrity and Efficiency was established as an independent entity within the executive branch to address integrity, economy, and effectiveness issues that transcend individual Government agencies. The PRAC is composed of Federal Offices of Inspector General to promote transparency and support and conduct oversight of congressionally provided funds to address the COVID-19 pandemic.

[7] FAR 15.404-1, "Proposal Analysis Techniques."

[8] An IGCE is an estimate of the expected cost of a contract or task order developed by Government personnel before soliciting contractor proposals or making contract awards.

Identifying and Mitigating Known Cybersecurity Risks

A key component to reducing cybersecurity risk is identifying and mitigating known cybersecurity vulnerabilities before deploying information technology products across the DoD's systems and networks. DoD Components can manage and reduce the cybersecurity risks associated with cyber vulnerabilities by developing and implementing risk mitigation strategies that include plans to identify and mitigate vulnerabilities when information technology products are deployed. The plans should include the use of automated scanning tools to identify known cybersecurity vulnerabilities, and a process for mitigating actions, such as patches, to address known vulnerabilities.[9] Connecting information technology products to the DoD Information Network (DODIN) without mitigating known cybersecurity risks can introduce cybersecurity vulnerabilities into DoD systems and networks.

The DoD Chief Information Officer requires DoD Components to review the DODIN Approved Products List (APL) before purchasing information technology products for unified capabilities.[10] The Defense Information Systems Agency (DISA) approves information technology products for use across the DoD and lists them on the DODIN APL. For information technology products other than those for unified capabilities, DoD Components may review and select products from various DoD Component-level APLs or procure products from approved vendors.

DoD Components must configure information technology products in accordance with applicable DISA Security Technical Implementation Guides (STIGs), Security Requirements Guides, or configuration guides before connecting to the network. DoD Components may use the Assured Compliance Assessment Solution (ACAS) automated tool to ensure compliance with DISA STIGs before the product is deployed. ACAS is a vulnerability scanning tool used to assess DoD networks and connected information technology products to identify known cybersecurity vulnerabilities.[11] DoD Component officials are required to develop mitigation strategies for any identified cybersecurity vulnerabilities in a plan of action and milestones (POA&M). POA&Ms must be maintained throughout the life cycle of the information technology product, and be updated as necessary to address any additional vulnerabilities.

[9] Patches are software code fixes that can correct security and functionality problems in software and firmware, as well as add new features, including security capabilities.

[10] DoD Instruction 8100.04, "Unified Capabilities," December 9, 2010. Unified capabilities are the integration of voice, video, and data services delivered across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness.

[11] Joint Force Headquarters-Department of Defense Information Network, Tasking Order 20-0020, "Assured Compliance Assessment Solution (ACAS) Operational Guidance," May 6, 2020.

Federal Requirements for Reporting Funding Used in Response to COVID-19

The CARES Act requires Federal agencies to accurately track and regularly report the use of CARES Act funds. OMB Memorandum M-20-21 allows agencies to meet the CARES Act reporting requirements by modifying existing reporting processes established under the Federal Funding Transparency Act, as amended by the Digital Accountability and Transparency Act (DATA Act).[12] Under the DATA Act, Federal agencies are required to submit their spending and contract and grant award data to USAspending.gov quarterly.

OMB Memorandum M-20-21 requires agencies to use newly established codes in their DATA Act submission to indicate whether contract actions were awarded in response to the COVID-19 pandemic and whether the spending and contract and grant award data are associated with supplemental funding (such as CARES Act funding), expenditures, or both. One of the new codes is the National Interest Action (NIA) Code—P20C, which identifies contract actions that directly support operations in response to the COVID-19 pandemic. The P20C NIA Code is assigned to the contract action regardless of the funding source, as DoD Components used CARES Act and other funding sources for those contract actions. USAspending.gov allows users to sort contract actions to specifically identify the actions associated with the COVID-19 pandemic.

Contract Actions Reviewed

From February 1, 2020, through May 13, 2020, the DoD awarded 367 contract actions worth $849 million to procure information technology products and services to support operations in response to the COVID-19 pandemic.[13] We initially selected a nonstatistical sample of 30 of those contract actions to review. The 30 contract actions—awarded by the Army, Navy, Air Force, Defense Health Agency (DHA), and DISA—had a total contract value of $94.3 million. Of those 30 contract actions, 2 had NIA codes indicating that they were awarded in response to the COVID-19 pandemic. However, Army and DISA contracting officials improperly coded these contract actions. Therefore, we reduced our sample to the remaining 28 contract actions, valued at $81.5 million. See Appendix B for a list of all contracts, by DoD Component, included in our sample.

[12] OMB Memorandum M-20-21, "Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019 (COVID-19)," April 10, 2020. Public Law 109-282, "Federal Funding Accountability and Transparency Act of 2006," September 26, 2006, amended by Public Law 113-101, "Digital Accountability and Transparency Act of 2014," May 9, 2014.

[13] Contract actions include contracts, contract modifications, and orders from contracts.

Review of Internal Controls

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.[14] The Army, Navy, Air Force, DHA, and DISA internal controls over the procurement of information technology products and services to support operations in response to the COVID-19 pandemic were effective as they applied to the audit objectives.

[14] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, Incorporating Change 1, Effective June 30, 2020.

Finding

DoD Components Procured, Assessed, and Reported Information Technology Products and Services in Accordance With Federal and DoD Requirements

The Army, Navy, Air Force, DHA, and DISA procured information technology products and services in accordance with the CARES Act and other Federal and DoD requirements. Specifically, for the 28 contract actions reviewed, the DoD Components:

- procured information technology products and services to support operations in response to the COVID-19 pandemic;
- paid fair and reasonable prices for products and services procured;
- assessed whether known cybersecurity risks existed and developed risk mitigation strategies for the risks before procuring or using the information technology products; and
- accurately reported the required COVID-19-related codes to USAspending.gov.

As a result, DoD stakeholders have assurance that the Army, Navy, Air Force, DHA, and DISA procured $81.5 million in information technology products and services in response to the COVID-19 pandemic at reasonable prices and reduced the risk of cybersecurity vulnerabilities associated with those procurements. Continued DoD efforts to comply with the CARES Act and other Federal and DoD requirements will reduce the risk of waste, fraud, and abuse associated with the procurement of the information technology products and services and ensure that the American public has visibility of DoD spending on contract actions associated with the response to COVID-19. Furthermore, continued DoD efforts to identify and mitigate cybersecurity vulnerabilities before procuring or using the information technology products and services will reduce the risk of introducing vulnerabilities into DoD systems and networks that could potentially jeopardize the DoD's missions, information, and assets.

DoD Components Procured Information Technology Products and Services to Support Operations in Response to the COVID-19 Pandemic

The Army, Navy, Air Force, DHA, and DISA procured information technology products and services to support operations in response to the COVID-19 pandemic for each of the 28 contracts we reviewed. The CARES Act requires the DoD to use the funding provided to prevent, prepare for, and respond to COVID-19. To determine

whether the contracts were awarded to support the DoD's response to the COVID-19 pandemic, we reviewed contract documentation, such as justification and approvals for other than full and open competition and price negotiation memorandums, for each of the 28 contract actions to identify how the products or services would be used in the DoD's response. For example, a Naval Information Warfare Systems Command contracting officer awarded a contract action for $2.2 million to rapidly acquire hardware upgrades that would allow users to access e-mail remotely via Outlook Web Access. The upgrades prevented mission degradation, maintained operational readiness, and ensured that users had consistent and reliable e-mail access during maximum telework. In another example, an Air Force Research Laboratory contracting officer awarded a contract action for $2.1 million to acquire laptops to support remote access to the Secret Internet Protocol Router Network for senior Air Force leadership. Furthermore, a DHA contracting officer awarded a contract action for $4.9 million for obtaining information technology services, including access to a Medical Logistics COVID-19 Response Platform that would provide remote access to data, response planning, and lessons learned in support of the DHA's Medical Logistics Directorate.

DoD Components Paid Fair and Reasonable Prices to Procure Information Technology Products and Services

The Army, Navy, Air Force, DHA, and DISA paid fair and reasonable prices to procure information technology products and services for the 28 contract actions we reviewed. In accordance with FAR requirements, the contracting officials conducted a price analysis to support documented price reasonableness determinations and prepared price negotiation memorandums for each contract action.[15] For each price analysis, contracting officials considered prices offered by vendors for information technology products and services and compared the proposed prices to ensure the agreed-to price was fair and reasonable.

The FAR and DFARS require contracting officers to evaluate the reasonableness of proposed prices from vendors, and document their price analysis to ensure the agreed-to price is fair and reasonable.[16] For the 28 contract actions that we reviewed, contracting officials used FAR price analysis techniques and compared the vendor's proposed price to one or a combination of the following categories.

- Multiple competitive quotes
- Historical prices paid

[15] Contracting officials included contracting officers, contracting specialists, and contracting branch and division chiefs.

[16] FAR 15.402, "Pricing policy"; FAR 15.404-1(a)(1), "Proposal Analysis Techniques"; and DFARS 215.371-3, "Fair and Reasonable Price and the Requirement for Additional Cost or Pricing Data."

- Published price lists
- IGCEs
- Prices obtained by conducting market research

For example, an Army contracting officer awarded a contract, valued at $800,000, for wireless devices to support U.S. Army Corps of Engineers teleworkers. In accordance with FAR proposal analysis techniques, the contracting officer conducted market research to determine whether current market trends affected the price, and compared the selected vendor's quote to an IGCE. In another example, an Air Force contracting officer awarded a contract action, valued at $1.1 million, for artificial intelligence-driven threat and risk assessment capabilities to enable the Commander of U.S. Northern Command to identify COVID-19 hotspots. In accordance with FAR proposal analysis techniques, the contracting officer compared the proposed price to published price lists and selected the significantly lower proposed price. Furthermore, a DISA contracting officer awarded a contract, valued at $1.2 million, to purchase hardware and parts to establish communication suites for U.S. Army North's COVID-19 response. DISA received two quotes that the contracting officer deemed technically acceptable. In accordance with FAR proposal analysis techniques, DISA contracting officials compared the competitive quotes and selected the quote that was the lowest price and technically acceptable. Table 1 summarizes the price analysis techniques that the DoD Components used to determine price reasonableness for each contract action we reviewed.

Table 1. Price Analysis Techniques Contracting Officials Used to Evaluate Price Reasonableness for Each Contract Action We Reviewed

	Contract Number	Date Awarded	Award Amount	FAR 15.404-1(b)(2) Price Analysis, Comparing Price to:				
				Competitive Quotes	Historical Prices	Price Lists	IGCE	Market Research Prices
ARMY								
1	W91QVN-20-F-02B4	April 1, 2020	$823,348.96				X	X
2	W912DY-19-F-0043	May 4, 2020	880,753.60				X	X
3	W912DY-19-F-0044	May 4, 2020	1,139,792.00				X	X
	Subtotal (3)		**$2,843,894.56**					
NAVY								
4	N00039-20-F-9705	March 20, 2020	905,984.60		X	X		X
5	N00039-20-F-9708	March 27, 2020	2,220,018.08			X		X
6	N00039-20-F-9711	April 16, 2020	2,999,854.40		X	X		
7	N00039-20-F-0237	April 22, 2020	2,949,502.00			X	X	
8	N00039-20-F-9714	April 23, 2020	1,778,376.95			X		X
9	N00039-20-F-9715	April 24, 2020	5,650,001.98		X			X
	Subtotal (6)		**$16,503,738.01**					
AIR FORCE								
10	FA8751-20-F-0034	April 3, 2020	2,130,410.00	X	X			
11	FA8726-20-F-0081	April 3, 2020	3,676,166.69				X	
12	FA2595-20-F-0007	April 16, 2020	4,366,600.00			X		X
13	FA2595-20-C-0002	April 16, 2020	1,100,000.00			X		
14	FA2595-20-C-0003	April 18, 2020	2,250,000.00			X		
15	FA2595-20-F-0008	April 27, 2020	2,212,661.47		X	X		X
16	FA2595-20-F-0011	May 8, 2020	2,343,504.00			X		X
	Subtotal (7)		**$18,079,342.16**					

Table 1. Price Analysis Techniques Contracting Officials Used to Evaluate Price Reasonableness for Each Contract Action We Reviewed (cont'd)

	Contract Number	Date Awarded	Award Amount	FAR 15.404-1(b)(2) Price Analysis, Comparing Price to:				
				Competitive Quotes	Historical Prices	Price Lists	IGCE	Market Research Prices
DEFENSE HEALTH AGENCY								
17	HT0015-20-C-0005	March 30, 2020	6,655,500.00	X		X	X	X
18	HT9402-20-F-0013	April 3, 2020	4,854,006.96	X	X		X	X
19	HT0015-20-P-0013	April 9, 2020	5,174,325.50	X		X	X	X
	Subtotal (3)		**$16,683,832.46**					
DEFENSE INFORMATION SYSTEMS AGENCY								
20	HC1013-15-F-C870	March 27, 2020	1,755,543.17	N/A*				
21	HC1013-20-F-C493	April 1, 2020	1,235,911.50		X	X	X	
22	HC1013-20-F-C547	April 9, 2020	815,595.59		X	X	X	
23	HC1028-20-F-0427	April 21, 2020	2,626,516.42	X		X	X	
24	HC1028-20-F-0438	April 23, 2020	9,872,510.00	X				
25	HC1028-20-F-0522	May 1, 2020	2,446,621.38	X		X		
26	HC1028-20-F-0527	May 4, 2020	1,220,154.40	X		X	X	
27	HC1028-20-F-0532	May 8, 2020	5,433,419.63	X		X	X	
28	HC1084-20-F-0177	May 12, 2020	1,937,760.00			X	X	
	Subtotal (9)		**$27,344,032.09**					
	Overall Total (28)		**$81,454,839.28**					

* The DISA contract action HC1013-15-F-C870 was awarded through a General Services Administration indefinite-delivery indefinite-quantity contract and, therefore, did not require DISA contracting officials to conduct a fair and reasonable price determination.

Source: The DoD OIG.

DoD Components Assessed Information Technology Products for Vulnerabilities and Developed Risk Mitigation Strategies

Army, Navy, Air Force, DISA, and DHA officials procured information technology products from approved sources, such as APLs or approved contractors; assessed cybersecurity vulnerabilities before using the products; and configured the products in accordance with DISA STIGs, Security Requirement Guides, and DoD Component-specific configuration guides. In addition, DoD Component cybersecurity officials developed risk mitigation strategies, when needed, to address known cybersecurity risks linked to the procured information technology products.[17]

The DoD Chief Information Officer requires DoD Components to review APLs and procure authorized information technology products for use within the DODIN.[18] In addition, Federal standards and DoD policies require cybersecurity officials to comply with applicable configuration management processes.[19] DoD Instruction 8510.01 requires DoD Components to configure information technology products in accordance with DISA STIGs and Security Requirement Guides and use automated vulnerability assessment tools to monitor information technology continuously to identify cybersecurity vulnerabilities; and develop and maintain POA&Ms to address known vulnerabilities. Furthermore, DoD Instruction 8500.01 requires DoD Components to identify, mitigate, and monitor risks associated with global sourcing and distribution; weaknesses or flaws inherent in information technology products; and vulnerabilities introduced through faulty design, configuration, or use.[20]

To determine whether the information technology products acquired were listed in APLs and authorized for use on the DODIN, we reviewed contract files and procurement information. We also reviewed configuration guides and STIG compliance reports, and held discussions with cybersecurity officials to determine whether information technology products were configured in accordance with DoD policy. In addition, we reviewed scan results from automated vulnerability assessment tools, such as ACAS, to verify that the DoD Components deployed automated tools to identify known cybersecurity risks affecting the procured

[17] Cybersecurity officials interviewed included cyber division chiefs and deputies, and information technology contractor support.

[18] DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010.

[19] National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 5, September 23, 2020. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, Incorporating Change 2, July 28, 2017.

[20] DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, Incorporating Change 1, Effective October 7, 2019.

products. We also reviewed the National Vulnerability Database and vendor websites to identify known cybersecurity risks associated with the procured products.[21] Lastly, we reviewed POA&Ms and actions taken by DoD Components to determine whether they mitigated the known vulnerabilities or reduced risk to an acceptable level.

The Army, Navy, Air Force, DHA, and DISA reduced the risk of introducing cybersecurity vulnerabilities in DoD systems and networks for the procured information technology products. For example, Navy contracting officials procured software services such as Microsoft Office 365 and Outlook Web Access—approved for use on the Navy's systems and networks—to expand Navy personnel telework capabilities.[22] Navy cybersecurity officials used ACAS to identify any cyber vulnerabilities associated with the software products and continuously monitored the Navy systems and networks by conducting biweekly ACAS scans as part of their risk mitigation efforts. Additionally, Navy cybersecurity personnel patched vulnerabilities identified by ACAS and conducted additional scans to ensure that the vulnerabilities affecting the Navy's network and the procured software services were remediated.

Air Force contracting officials procured Dell Latitude 5501 laptops from an approved vendor. These laptops were authorized for use on the DODIN, and Air Force senior leaders used them to securely connect to various DoD networks remotely. Air Force cybersecurity officials provided a copy of the baseline configuration requirements and stated that the laptops were configured in accordance with Air Force configuration guides. Air Force cybersecurity officials provided the ACAS vulnerability scan reports that they used to identify known cybersecurity risks affecting the information technology products. In addition, Air Force cybersecurity officials implemented mitigating security controls to prevent unauthorized users from exploiting cyber vulnerabilities to access, make configuration changes, or take control of the procured computers. We reviewed documentation supporting that security patches were installed to address some of the cyber vulnerabilities as well as documentation supporting the security measures put in place for cyber vulnerabilities that remained. The Air Force authorizing official reviewed the security posture, identified risks, system requirements, and security countermeasures and determined that a satisfactory level of security was present for operations. We reviewed the authorization documents that provided authority for the laptops to be used on the DODIN.

[21] The National Vulnerability Database is the U.S. Government repository of cybersecurity vulnerability management data, including security-related software flaws, misconfigurations, product names, and impact metrics.

[22] The Navy uses the "Department of the Navy Application and Database Management System," a web-enabled registry, to manage its portfolio of approved Marine Corps and Navy information technology applications.

DHA contracting officials awarded several contracts to procure laptops—HP ProBook 640 G4 and Dell 5400 Notebooks. Those laptops were authorized for use on the DODIN and were included on various APLs. In addition, DHA cybersecurity personnel configured the laptops in accordance with applicable Security Requirement Guides and STIGs and then validated compliance with the STIGs using the Security Content Automation Protocol (automated compliance checker). Furthermore, DHA cybersecurity personnel developed risk mitigation strategies to address cybersecurity threats for the procured laptop computers, including deploying ACAS to identify cybersecurity risks on information technology products.

DoD Components Accurately Reported the Required COVID-19-Related Codes

Army, Navy, Air Force, DHA, and DISA contracting officials accurately reported the NIA Code in the DoD FY 2020 second and third quarter DATA Act submissions for the 28 contracts we reviewed, in accordance with OMB Memorandum M-20-21. Specifically, the contracting officials used the NIA Code, P20C, to appropriately report that the 28 contract actions were in response to the COVID-19 pandemic. To confirm whether the DoD Components accurately reported the NIA Code, we reviewed the DoD FY 2020 second and third quarter DATA Act submissions. We then reviewed contract documentation for each of the 28 contract actions to determine whether the contracts were awarded to support the DoD's response to the COVID-19 pandemic.

DoD Stakeholders Have Assurance That Procurements Are At Reduced Risk for Waste, Fraud, and Abuse

As a result of the DoD's compliance with the CARES Act and other Federal and DoD requirements, DoD stakeholders have assurance that the Army, Navy, Air Force, DHA, and DISA procured $81.5 million in information technology products and services in response to the COVID-19 pandemic at reasonable prices and at a reduced risk of cybersecurity vulnerabilities. In June 2020, the PRAC identified financial management of CARES Act funding as one of the top management and performance challenges.[23] According to the PRAC, the substantial increases in money allocated for certain programs and the expedited timetable for distribution of CARES Act and other pandemic-related funds have heightened concerns about existing management control weaknesses and increased the risk of misuse and fraud. Those heightened concerns and increased risk make it imperative that the DoD continues to comply with the CARES Act and other Federal and DoD requirements.

[23] Council of the Inspectors General on Integrity and Efficiency, Pandemic Response Accountability Committee, "Top Challenges Facing Federal Agencies: COVID-19, Emergency Relief and Response Efforts," June 2020.

Specifically, continued DoD efforts to comply with the CARES Act and other Federal and DoD requirements will reduce the risk of waste, fraud, and abuse associated with the procurement of the information technology products and services and ensure that the American public has visibility of DoD spending on contract actions associated with the response to COVID-19. Furthermore, continued DoD efforts to identify and mitigate cybersecurity vulnerabilities before procuring or using the information technology products and services, will reduce the risk of introducing vulnerabilities into DoD systems and networks that could potentially jeopardize DoD's missions, information, and assets.

Other Matters of Interest

As stated in the Background section of this report, we did not include 2 of the 30 initial contract actions in our nonstatistical sample in our review. Army and DISA contracting officials improperly coded the two contract actions as being awarded in response to the COVID-19 pandemic. We notified the Army and DISA contracting officials that the contracts were improperly coded, and they took immediate action to delete the NIA Code. Specifically, contracting officials from U.S. Army Mission and Installation Contracting Command–Fort Sam Houston corrected the miscoding for the contract action and implemented a corrective action plan to reduce the command's risk of miscoding future contract actions. DISA contracting officials corrected the miscoding for the DISA contract action. In addition, in July 2020, DISA updated its procurement review procedures to identify acquisitions related to COVID-19 and reduce the risk of miscoding future procurements. Neither the Army nor DISA used CARES Act funding for the incorrectly coded contract actions.

Appendix A

Scope and Methodology

We conducted this performance audit from May 2020 to January 2021 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 objective.

We reviewed the following legislation and other contracting guidance to identify specific requirements applicable to the DoD's use of funding, including supplemental funding, when supporting operations in response to the global COVID-19 pandemic.

- Public Law 116-136, "Coronavirus Aid, Relief, and Economic Security Act"
- Public Law 116-127, "Families First Coronavirus Response Act"
- Public Law 116-123, "Coronavirus Preparedness and Response Supplemental Appropriations Act"
- FAR Part 15, "Contracting by Negotiation," Subpart 15.404-1, "Proposal Analysis Techniques"

We used the Federal Procurement Data System–Next Generation to identify a universe of contract actions to review. From February 1, 2020, through May 13, 2020, the DoD awarded 367 contract actions to procure information technology products and services to support operations in response to the COVID-19 pandemic. We filtered the data for contract actions with a total value of $849 million that included product or service codes D300 (Information Technology and Telecom) and 7000 (Information Technology) awarded by DoD Components using the NIA Code to identify that the procurement was in response to the COVID-19 pandemic. We developed a nonstatistical sample of 35 contract actions. However, we excluded 7 of the 35 contract actions because:

- 4 contract actions would have resulted in a low impact to the audit based on the products or services procured or monetary value,
- 1 contract action was a modification to a contract already in the sample, and
- 2 contract actions were improperly coded but were not awarded in response to the COVID-19 pandemic.

We limited our reporting for the two miscoded contracts to confirming that the contract actions were not in response to the pandemic, that supplemental funding was not used, and that actions were taken to correct the coding and avoid future

improper coding. For the remaining 28 contracts, valued at $81.5 million, we analyzed contract documentation, including the contracts and modifications, price negotiation memorandums and supporting documentation, and justification and approval for other than full and open competition to determine whether the contracts were awarded in accordance with applicable laws and regulations.

In addition, we reviewed the contracts to determine whether the Army, Navy, Air Force, DHA, and DISA procured information technology products from trusted DoD suppliers and whether the products were included on the DODIN APL and Component-level APLs. We also identified whether contracts included products with known cybersecurity risks by reviewing vulnerabilities included in the National Vulnerabilities Database and vendor websites. For information technology products with known cybersecurity risks, we reviewed DoD Component cybersecurity risk mitigation strategies and actions taken to limit the risk to an acceptable level when those products were used in operational environments.

We obtained the financial and award data (Files A to D) for the FY 2020 second and third quarters that the DoD submitted for publication on USAspending.gov. We reviewed the procurement award data (File D1) and then identified the corresponding transactions for the 28 contracts in our sample to determine the DoD's accuracy of reporting the NIA Code, P20C, for the procurement award data.

We interviewed officials from the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer to identify additional DoD requirements for DoD Components that used CARES Act funds provided by Congress to support DoD operations in response to the COVID-19 pandemic. In addition, we interviewed contracting and cybersecurity officials to identify Component-specific guidance for managing the use of CARES Act funding. Specifically, we interviewed contracting officers, contracting specialists, contracting branch and division chiefs, internal review and audit compliance officials, and contracting officer's representatives to identify the price analysis techniques used to determine whether contract prices were fair and reasonable. Furthermore, we interviewed cyber division chiefs and deputies, information technology contractor support personnel, and the DISA Deputy Risk Management Executive to identify risk mitigation strategies and actions taken by DoD Components to address known cybersecurity risks linked to the procured information technology products. Those officials represented:

- U.S. Army Contracting Command;
- U.S. Army Corps of Engineers Engineering and Support Center;
- Assistant Secretary of the Navy (Research, Development, and Acquisition);
- Air Force Materiel Command;
- DHA; and
- DISA.

Use of Computer-Processed Data

We relied on computer-processed data from the Federal Procurement Data System–Next Generation to identify contracts used to procure information technology products and services to support operations in response to the COVID-19 pandemic. We also used the contracts from the Federal Procurement Data System–Next Generation to develop a nonstatistical sample of contracts included in the audit. The data we obtained from the Federal Procurement Data System–Next Generation were not the basis for our conclusions or findings. To assess the accuracy of the data obtained, we verified the Federal Procurement Data System–Next Generation data against official contract records. We determined that the data were sufficiently reliable for identifying contracts to develop a nonstatistical sample.

Use of Technical Assistance

The DoD Office of Inspector General (DoD OIG) Quantitative Methods Division assisted with developing the nonstatistical sample of contracts included in the audit.

Prior Coverage

During the last 5 years, the Council of the Inspectors General on Integrity and Efficiency, PRAC, Government Accountability Office (GAO), and the DoD OIG issued six reports discussing COVID-19 pandemic response and procurement of information technology products and services. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

Council of the Inspectors General on Integrity and Efficiency, Pandemic Response Accountability Committee

"Top Challenges Facing Federal Agencies: COVID-19 Emergency Relief and Response Efforts," June 17, 2020

> The CARES Act and other related legislation provided more than $2.4 trillion in Federal spending to address the public health and economic crisis resulting from the COVID-19 pandemic. In an effort to promote transparency and support oversight, the PRAC issued this report to provide insight into the top management challenges facing Federal agencies that received emergency funds in response to COVID-19 as identified by Offices of Inspector General from 37 agencies. Among other challenges, the PRAC identified challenges such as financial management, and information technology security and management.
>
> Within financial management, the PRAC identified concerns with the ability of agencies to track and report financial data due to internal controls and outdated financial management systems. In addition, the PRAC identified

critical issues with the ability of Federal agencies to prevent and reduce improper payments under statutory, contractual, or legally applicable requirements, including ineligible receipts, duplicative payments, or payments not supported by documentation.

Within information technology security and management, the PRAC identified concerns related to the widespread reliance on maximum telework to continue agency operations during the COVID-19 pandemic, which has strained agency networks, shifted information technology resources, and introduced additional opportunities and targets for cyber attacks created by increased remote access to networks.

GAO

GAO-20-632, "COVID-19 Contracting: Observations on Federal Contracting in Response to the Pandemic," July 29, 2020

The CARES Act included a provision for the GAO to provide a comprehensive review of COVID-19 Federal contracting. This report describes, among other objectives, key characteristics of Federal contracting obligations awarded in response to the COVID-19 pandemic.

The GAO analyzed Federal Procurement Data System-Next Generation data on agencies' reported Government-wide contract obligations for COVID-19 through June 11, 2020. The GAO also analyzed contract obligations reported at the Departments of Health and Human Services, Defense, Homeland Security, and Veterans Affairs – the highest obligating services. Based on data in the Federal Procurement Data System-Next Generation, Government-wide contract obligations in response to the COVID-19 pandemic totaled about $17.8 billion as of June 11, 2020. Across the 42 Federal departments and agencies with COVID-19 contract obligations, the Departments of Health and Human Services, Defense, Homeland Security, and Veterans Affairs accounted for 85 percent of total contract obligations.

DoD OIG

Report No. DODIG-2020-060, "Audit of Contract Costs for Hurricane Recovery Efforts at Navy Installations," February 12, 2020 (Report is FOUO)

The DoD OIG determined that Naval Facilities Engineering Command (NAVFAC) Southeast contracting officials did not control costs when awarding and administering the Global Contingency Construction-Multiple Award Contract task order issued to recover Naval Air Station Key West after Hurricane Irma. This occurred because the NAVFAC Southeast contracting officials chose not

to implement NAVFAC contracting procedures when planning, awarding, and administering the task order for the initial recovery work. As a result, without a cost proposal or documentation of NAVFAC Southeast's determination of fair and reasonable prices for the initial $9.3 million of the $35.9 million hurricane recovery, the DoD OIG could not verify that the NAVFAC Southeast contracting officials obtained fair and reasonable prices. Furthermore, the procedures that NAVFAC Southeast used may have created an illegal cost-plus-percentage-of-cost contracting system that did not incentivize the contractor to complete the contract efficiently or effectively.

Report No. DODIG-2019-106, "Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items," July 26, 2019 (Report is SECRET//NOFORN)

The DoD OIG determined that the DoD purchased and used commercial off-the-shelf (COTS) information technology items with known cybersecurity risks. Specifically, Army and Air Force Government purchase card holders purchased at least $32.8 million of COTS information technology products with known cybersecurity vulnerabilities in FY 2018. The DoD purchased and used COTS information technology items with commonly known cybersecurity risks because the DoD did not establish:

- responsibility for an organization or group to develop a strategy to manage the cybersecurity risks of COTS information technology items;
- acquisition policies that proactively address the cybersecurity risks of COTS information technology items;
- an APL to prevent unsecure items from being purchased; and
- controls to prevent the purchase of high-risk COTS information technology items with known cybersecurity risks similar to the controls implemented through the use of the national security systems-restricted list.

If the DoD continues to purchase and use COTS information technology items without identifying, assessing, and mitigating the known vulnerabilities associated with these items, missions critical to national security could be compromised.

Report No. DODIG-2019-060, "Review of Parts Purchased from TransDigm Group, Inc.," February 25, 2019 (Report is FOUO)

The DoD OIG determined that TransDigm earned excess profit on 46 of 47 parts purchased by the Defense Logistics Agency and Army, even though contracting officers followed the FAR and the DFARS when they determined that prices were fair and reasonable for the 47 parts at the time of the contract award.

TransDigm was charging excess profit because prices for parts had become inflated over time, and TransDigm was the only manufacturer for the majority of the parts competitively awarded. In addition, statutory and regulatory requirements discouraged contracting officers from asking for uncertified cost data when determining whether a price was fair and reasonable. The DoD OIG determined that TransDigm earned $16.1 million in excess profit for 46 parts it sold to the Defense Logistics Agency and Army between January 2015 and January 2017. Furthermore, the DoD OIG determined that the DoD could continue paying excess profits on parts purchased from sole-source manufacturers and providers of spare parts if statutory and regulatory requirements continue to discourage contracting officers from requesting uncertified cost data and allow contractors to avoid providing uncertified cost data when requested.

Report No. DODIG-2017-112, "Defense Organizations Price Reasonableness Determinations for Federal Supply Schedule Orders for Supplies," August 15, 2017

The DoD OIG determined that the Washington Headquarters Services, DoD Human Resources Activity, and Defense Threat Reduction Agency contracting officers made adequate price reasonableness determinations for 10 orders, valued at $7.7 million. However, the Washington Headquarters Services, DoD Human Resources Activity, DHA, and Defense Threat Reduction Agency contracting officers did not adequately document and support whether the prices paid for 47 orders, valued at $40.3 million, were fair and reasonable. The Washington Headquarters Services, DoD Human Resources Activity, DHA, and Defense Threat Reduction Agency contracting officers did not adequately document and support reasonableness and fairness in prices paid for 47 orders because of time constraints, lack of oversight, and turnovers with contracting officers. In addition, the Defense Procurement and Acquisition Policy Director, Washington Headquarters Services, DoD Human Resources Activity, DHA, and Defense Threat Reduction Agency management did not issue guidance or provide training to contracting officers related to price reasonableness determinations and price analysis for orders of commercial supplies. As a result, the Washington Headquarters Services, DoD Human Resources Activity, DHA, and Defense Threat Reduction Agency customers may have paid more than they should have for supplies purchased.

Appendix B

Information Technology Products and Services Contracts Awarded in Response to the COVID-19 Pandemic

The DoD awarded more than 300 information technology products and services contracts, in response to the COVID-19 pandemic, from February 1, 2020, through May 13, 2020. We reviewed 28 contract actions for information technology products and services awarded in response to the pandemic, with a total award amount of $81.5 million. See Table 2 for a list of all contract actions, by DoD Component, included in our sample.

Table 2. Contract Actions Reviewed for Information Technology Products and Services Procured by DoD Components in Response to the COVID-19 Pandemic

	Contract Number	Modification/ Order Number	DoD Component	Date Awarded	Award Amount
1	W91QVN-20-F-02B4		Army	April 1, 2020	$823,348.96
2	W912DY-19-F-0043	P00003	Army	May 4, 2020	880,753.60
3	W912DY-19-F-0044	P00003	Army	May 4, 2020	1,139,792.00
4	N00039-20-F-9705		Navy	March 20, 2020	905,984.60
5	N00039-20-F-9708		Navy	March 27, 2020	2,220,018.08
6	N00039-20-F-9711		Navy	April 16, 2020	2,999,854.40
7	N00039-20-F-0237		Navy	April 22, 2020	2,949,502.00
8	N00039-20-F-9714		Navy	April 23, 2020	1,778,376.95
9	N00039-20-F-9715		Navy	April 24, 2020	5,650,001.98
10	FA8751-20-F-0034		Air Force	April 3, 2020	2,130,410.00
11	FA8726-20-F-0081		Air Force	April 3, 2020	3,676,166.69
12	FA2595-20-F-0007		Air Force	April 16, 2020	4,366,600.00
13	FA2595-20-C-0002		Air Force	April 16, 2020	1,100,000.00
14	FA2595-20-C-0003		Air Force	April 18, 2020	2,250,000.00
15	FA2595-20-F-0008		Air Force	April 27, 2020	2,212,661.47
16	FA2595-20-F-0011		Air Force	May 8, 2020	2,343,504.00
17	HT0015-20-C-0005		DHA	March 30, 2020	6,655,500.00
18	HT9402-20-F-0013		DHA	April 3, 2020	4,854,006.96
19	HT0015-20-P-0013		DHA	April 9, 2020	5,174,325.50
20	HC1013-15-F-C870		DISA	March 27, 2020	1,755,543.17

Table 2. Contract Actions Reviewed for Information Technology Products and Services Procured by DoD Components in Response to the COVID-19 Pandemic (cont'd)

	Contract Number	Modification/ Order Number	DoD Component	Date Awarded	Award Amount
21	HC1013-20-F-C493		DISA	April 1, 2020	1,235,911.50
22	HC1013-20-F-C547		DISA	April 9, 2020	815,595.59
23	HC1028-20-F-0427		DISA	April 21, 2020	2,626,516.42
24	HC1028-20-F-0438		DISA	April 23, 2020	9,872,510.00
25	HC1028-20-F-0522		DISA	May 1, 2020	2,446,621.38
26	HC1028-20-F-0527		DISA	May 4, 2020	1,220,154.40
27	HC1028-20-F-0532		DISA	May 8, 2020	5,433,419.63
28	HC1084-20-F-0177		DISA	May 12, 2020	1,937,760.00
	Total				**$81,454,839.28**

Source: The DoD OIG.

Acronyms and Abbreviations

ACAS	Assured Compliance Assessment Solution
APL	Approved Products List
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
COTS	Commercial Off-The-Shelf
COVID-19	Coronavirus Disease–2019
DATA Act	Digital Accountability and Transparency Act
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Systems Agency
DODIN	DoD Information Network
FAR	Federal Acquisition Regulation
IGCE	Independent Government Cost Estimate
NAVFAC	Naval Facilities Engineering Command
NIA	National Interest Action
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
PRAC	Pandemic Response Accountability Committee
STIG	Security Technical Implementation Guide


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

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