Defense Information Systems Agency
Working Capital Fund
Agency Financial Report
Fiscal Year 2021

Message from the Defense Information Systems Agency

As director of the Defense Information Systems Agency (DISA), I am pleased to present the Annual Financial Report (AFR) for the DISA Working Capital Fund, as of Sept. 30, 2021. The AFR financial statements and accompanying footnotes also include Management Discussion and Analysis and a Performance and Financial Section, which contain the auditor's signed report. The AFR is prepared as directed by Office of Management and Budget (OMB), Circular A-136.

DISA's mission supports the warfighter, while also consistently posturing itself in everyday operations and execution of its mission to promote the department's goal to achieve auditable financial statements. The agency endeavors to be a trusted provider to its mission partners, as well as to provide a distinct position of trust to the American people. DISA engages in modernization to improve the security, resiliency, and capacity for sound infrastructure and to ensure DoD networks achieve greater performance and affordability in a secure, integrated, and improved environment. As a vital part of infrastructure, audit is embedded in the agency from a top-down and bottom-up enterprise-wide undertaking engaging the DISA workforce.

DISA executed its internal control program in accordance with the OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control"; and the Green Book, GAO-14-704G, "Standards for Internal Control in the Federal Government." DISA can provide reasonable assurance that internal controls over operations and compliance are operating effectively as of Sept. 30, 2021. DISA is unable to provide assurance that internal controls over reporting are operating effectively as discussed in the AFR. DISA has executed actions to remedy inadequacies.

The agency continues to improve our structure to execute our strategy more effectively. This is accomplished by modernization; optimization; strengthening and driving innovation while promoting accountability; reducing duplication; and improving cost management.

ROBERT J. SKINNER
Lieutenant General, USAF
Director

Table of Contents

DISA Working Capital Fund Fiscal Year 2021

Management Discussion and Analysis

Defense Information Systems Agency (DISA) is pleased to present a Management Discussion and Analysis (MD&A) to accompany the financial statements and footnotes for its fiscal year (FY) 2021 financial statements. The key sections within this MD&A include the following:

1. **Mission and Organizational Structure**
2. **Performance Goals, Objectives, and Results**
3. **Analysis of Entity's Financial Statements**
4. **Management Discussion and Analysis of Systems, Controls, and Legal Compliance**
5. **Forward Looking**
6. **Limitations of the Financial Statements**

Elements of the report — such as DISA's organizational structure, ethos, and strategic plan — reflect DISA in FY 2021 and do not take into account updates and changes made starting in FY 2022.

1. Mission and Organizational Structure

History and Enabling Legislation

DISA, a combat support agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations. DISA implements the Secretary of Defense's Defense Strategic Guidance (DSG) and reflects the Department of Defense (DoD) Chief Information Officer's (CIO) Capability Planning Guidance (CPG). The DoD CIO vision is "to deliver an information dominant domain to defeat our nation's adversaries."

DISA serves the needs of the president, vice president, secretary of defense (SECDEF), Joint Chiefs of Staff (JCS), combatant commands (COCOMs), and other DoD components during peace and war. In short, DISA provides global net-centric solutions in the form of networks, computing infrastructure, and enterprise services to support information sharing and decision-making for the nation's warfighters and those who support them in the defense of the nation. DISA is charged with connecting the force by linking processes, systems, and infrastructure to people.

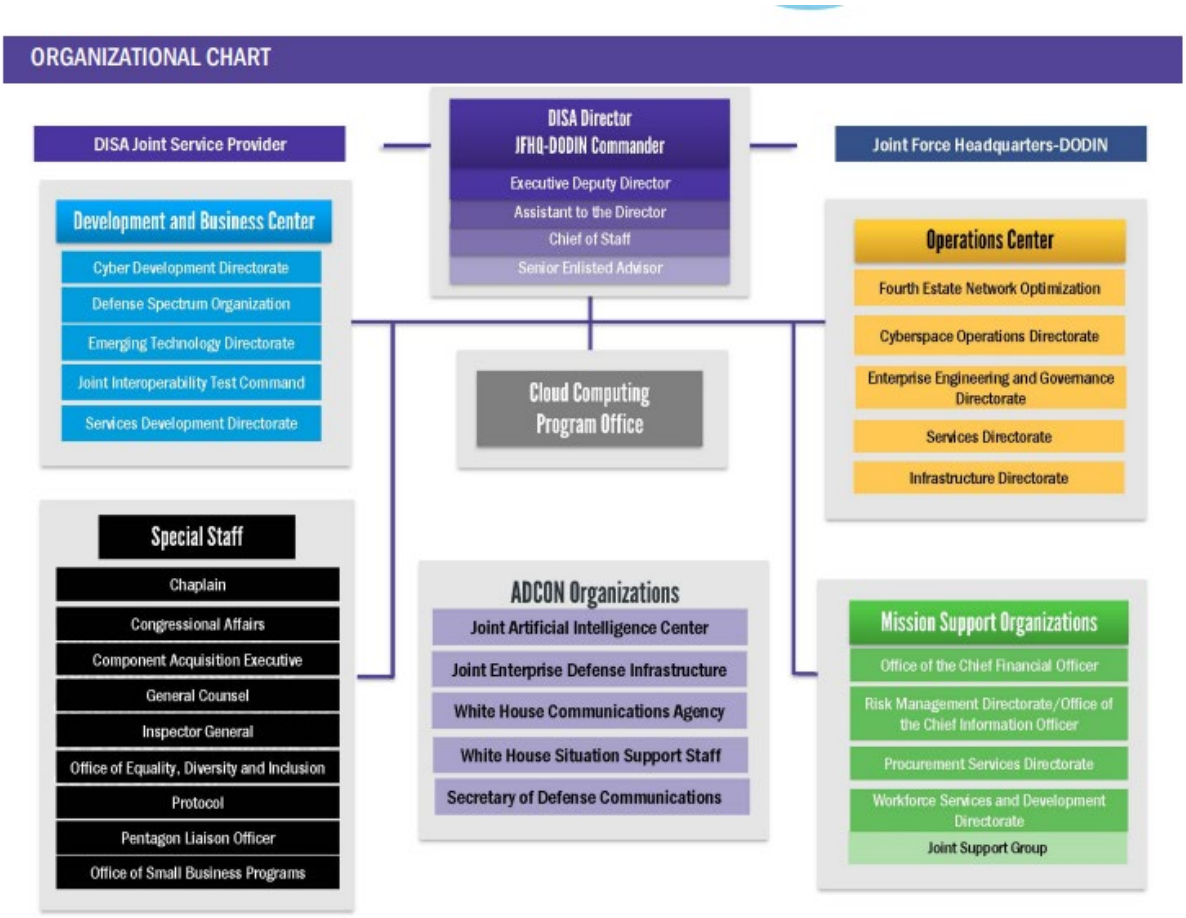
DISA's roots go back to 1959 when the JCS requested the SECDEF approve a concept for a joint military communications network to be formed by consolidation of the communications facilities of the military departments. This would ultimately lead to the formation of the Defense Communications Agency (DCA), established on May 12, 1960, with the primary mission of operational control and management of the Defense Communications System (DCS). On June 25, 1991, DCA underwent a major reorganization and was renamed the Defense Information Systems Agency to reflect its expanded role in implementing the DoD's Corporate Information Management (CIM) initiative and to clearly identify DISA as a combat support agency. DISA established the Center for Information Management to provide technical and program execution assistance to the assistant secretary of defense command, control, communications, and intelligence (C3I) and technical products and services to DoD and military components. In September 1992, DISA's role in DoD information management continued to expand with implementation of several Defense Management Report Decisions (DMRD), most notably DMRD 918.

DMRD 918 created the Defense Information Infrastructure (DII) and directed DISA to manage and consolidate the services' and DoD's information processing centers into 16 mega-centers. In FY 2018, the organization that came to be known as the Joint Service Provider (JSP) declared full operational capability and moved into its new place in the Defense Department's organizational chart as a subcomponent of DISA. It marked a major expansion of mission and budget authority for DISA, which now controls the funding and personnel that provide most information technology (IT) services for the Pentagon and other DoD headquarters functions in the National Capital Region. DISA continues to offer DoD information systems support, taking data services to the forward deployed warfighter.

DISA Mission, Vision, Ethos, Creed, and Core Values

Organization

To fulfill its mission and meet strategic plan objectives, DISA operates under the direction of the DoD CIO who reports directly to the secretary of defense. The organizational structure for DISA as of June 2021 is depicted below:



The agency is budgeted to support the IT needs and requirements of the entire Defense Department, including the offices of the secretary of defense and of the chairman and vice chairman of the Joint Chiefs of Staff, the Joint Staff, military services, combatant commands, and defense agencies. DISA also provides support to the White House and many federal agencies through a number of capabilities and initiatives.

DISA's Defense Working Capital Fund (DWCF)

DISA operates a Defense Working Capital Fund (DWCF) budget. The Working Capital Fund (WCF) relies on revenue earned from providing IT and telecommunications services and capabilities to finance specific operations. Mission partners order capabilities or services from DISA and make payment to the WCF when the capabilities or services are received.

A DWCF business unit is not profit-oriented and therefore, only tries to break even, charging prices set using the full-cost-recovery principle, which accounts for all costs — both direct and indirect (or "overhead") costs. It is intended to generate adequate revenue to cover the full cost of its operations and to finance the fund's continuing operations without fiscal year limitation.

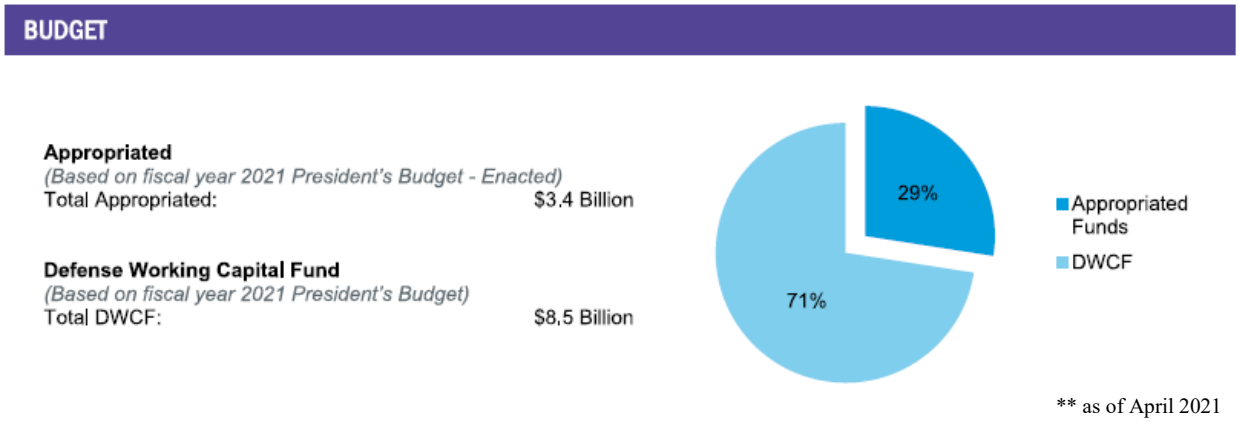
DISA operates the information services activity within the DWCF. This activity consists of two main components. The first component includes two lines of service: Telecommunications Services and Enterprise Acquisition Services (TSEAS). The second component includes Computing Services (CS).

The major element of the Telecommunication Services (TS) component is the Defense Information Systems Network (DISN), which provides interoperable telecommunications connectivity and accompanying services that allow the department to plan and operate both day-to-day business and operational missions through the dynamic routing of voice, data, text, still and full-motion imagery, and bandwidth services. Some DISN services are provided to mission partners in predefined packages and sold on a subscription basis via the DISN subscription service, while others are made available on a cost-reimbursable basis.

The line of service for enterprise acquisition services (EAS) enables the department to procure best value, commercially competitive IT services and capabilities through DISA's Defense IT Contracting Organization (DITCO). DITCO provides complete contracting support and services.

The computing services component of DISA's DWCF activities comprises the defense enterprise computing centers (DECCs), which provide mainframe and server-processing operations, data storage, production support, technical services, and end-user assistance for command and control, combat support, and enterprise applications across DoD. These facilities and functions provide a robust enterprise computing environment to more than 4 million users through 20 mainframes, more than 16,700 servers, 75,000 terabytes of data, and approximately 222,000 square feet of raised floor.

Resources: DISA is a combat support agency of the DoD with a $11.9 billion annual budget.



** as of April 2021

Global Presence

DISA is a global organization of approximately 6,500 civilian employees; approximately 1,500 active-duty military personnel from the Army, Air Force, Navy, and Marine Corps; and over 10,000 defense contractors. This data is as of June 30, 2021. DISA's headquarters is at Fort Meade, Maryland, and has a presence in 25 states and the District of Columbia within the United States, and in seven countries, and Guam (U.S. Territory), with 55 percent of its people based at Fort Meade and the National Capital Region (NCR), and 45 percent based in field locations. In addition, the following organizations are a part of DISA: Office of the Chief Financial Officer (OCFO), Component and Acquisition Executive (CAE), Development and Business Center (DBC), Chief of Staff, Inspector General (IG), Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), JSP, Operations Center (OC), Procurement Services Directorate (PSD), Risk Management Executive (RME), WHCA, and Workforce Services and Development Directorate (WSD). DISA provides a core enterprise infrastructure of networks, computing centers, and enterprise services (internet-like information services) that connect 4,300 locations, reaching 90 nations supporting DoD and national interests.

2. Performance Goals, Objectives, and Results

DISA is charged with the responsibility for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the president, the vice president, the secretary of defense, and the DoD components under all conditions of peace and war. The challenges faced by the department impact DISA directly in achieving success with respect to these responsibilities. DISA provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. DISA's number one priority is enabling information superiority for the warfighter and those who support them. Warfighters on all fronts require DISA's continued support because immediate connection, sharing, and assured access to information capabilities are essential to our mission partners' operational success.

DISA Strategic Goals and Objectives as outlined in the FY 2019-2022 Strategic Plan (Version 2) include:

Strategic Goals	Strategic Objectives
Operate and Defend	1.1 Modernize the Infrastructure 1.2 End User Support 1.3 Computing 1.4 Defensive Cyber Operations-Internal Defensive Measures Readiness
Adopt Before We Buy and Buy Before We Create	2.1 Optimize for the Enterprise 2.2 Strengthen Cybersecurity 2.3 Drive Innovation
Enable People and Reform the Agency	3.1 Enable People 3.2 Reform the Agency

DISA's strategic framework presents goals, objectives, and capabilities to support the agency's mission of conducting DODIN operations. DISA's goals that uphold the enduring mission include the following: to operate and defend; adopt before we buy and buy before we create; and enable people and reform the agency. The agency continues to augment and improve our structure to more effectively execute our strategy, by modernizing, optimizing, strengthening and driving innovation while promoting accountability, reducing duplication, and improving cost management.

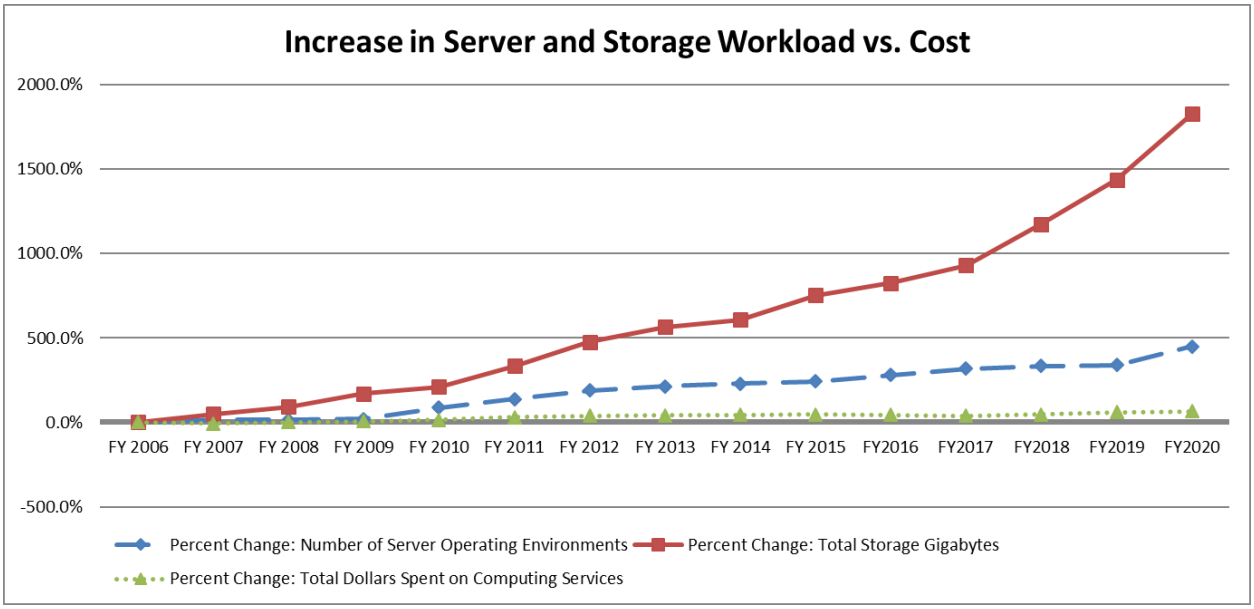
Program Performance

DISA's information services play a key role in supporting the DoD's operating forces. As a result, DISA is held to high performance standards. In many cases, performance measures are detailed in service-level agreements (SLAs) with individual customers that exceed the general performance measures discussed in the following paragraphs.

Computing Services Performance Measures

As shown in the subsequent table, demand for DISA's server and storage computing services has grown significantly since FY 2006. Since that year, the number of customer-driven server operating environments (OEs) has increased by 448 percent, and total storage gigabytes have increased by 1,828 percent. Over the same timeframe, the cost to deliver all computing services has increased by only 66

percent. In short, customers are demanding considerably more services and are at the same time benefiting from DISA's unique ability to leverage robust computing capacity at DISA data centers.



The Computing Service business area tracks its performance and results through the agency director's Quarterly Performance Reviews. There are two key operational metrics that are presented to the DISA director in conjunction with regular, recurring Quarterly Program Reviews. These two metrics depicted in the following tables reflect the availability of critical applications in the Core Data Centers. The first metric, "Core Data Center Availability," expressed in minutes per year, represents application availability from the end user's perspective and includes all outages or downtime regardless of root cause or problem ownership. Tier II requires achieving 99.75 percent availability, which limits downtime to approximately 1,361 minutes per year. Tier III, the standard for all DoD-designated Core Data Centers, requires achieving 99.98 percent availability, which limits downtime to approximately 95 minutes per year. The second metric, "Capacity Service Contract Equipment Availability," represents DISA's equipment availability by technology, i.e., how well DISA is executing its responsibilities exclusive of factors outside the agency's control such as last-mile communications issues, base power outages, or the like. The "Threshold" refers to system uptime and capacity availability for intended use; this is the level required by contract. The "Objective" is the value agreed on by the vendor and the government to be an ideal target, and the vendor reports the actual value on a monthly basis.

Core Data Center Availability

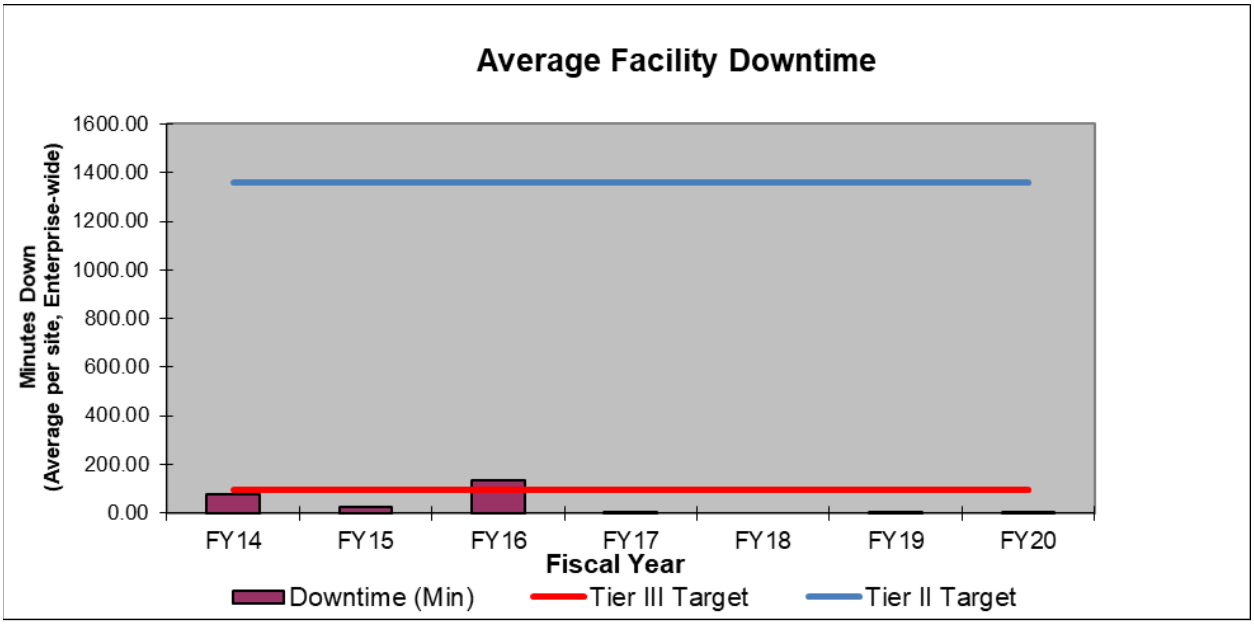


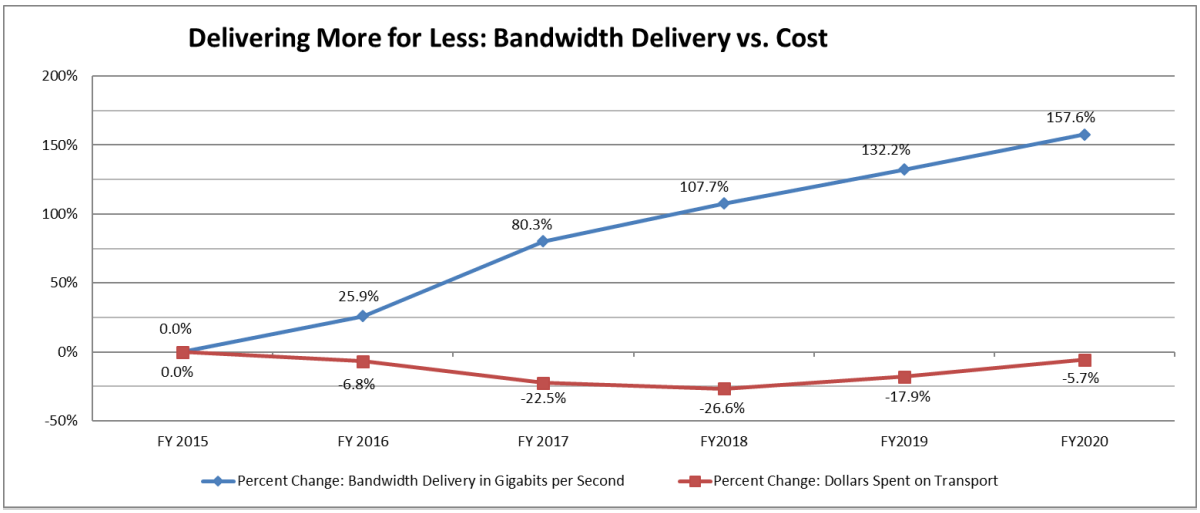
Figure 1- Capacity Service Contract Equipment Availability

	Threshold	Objective	Actual
IBM System z Mainframe	99.95%	99.99%	100%
Unisys Mainframe	99.95%	99.99%	100%
P Series Server	99.95%	99.99%	100%
SPARC Server	99.95%	99.99%	100%
X86 Server	99.95%	99.99%	99.999%
Itanium	99.95%	>99.95%	99.999%
Storage	99.95%	>99.95%	99.996%
Communications Devices	99.95%	>99.95%	99.999%

Telecommunications Services Performance Measures

The Telecommunications Services business area provides a set of high quality, reliable, survivable, and secure telecommunications services to meet the department's command and control requirements. The major component of Telecommunications Services is the DISN, a critical element of the DODIN that provides the warfighter with essential access to timely, secure, and operationally relevant information to ensure the success of military operations. The DISN is a collection of robust, interrelated telecommunications networks that provide assured, secure, and interoperable connectivity for the DoD, coalition partners, national senior leaders, combatant commands, and other federal agencies. Specifically, the DISN provides dynamic routing of voice, data, text, imagery (both still and full motion), and bandwidth services. The robustness of this telecommunications infrastructure has been demonstrated by DISA's repeated ability to meet terrestrial and satellite surge requirements in southwest Asia while supporting disaster relief and recovery efforts throughout the world. Overall, the DISN provides a lower

customer price through bulk quantity purchases, economies of scale, and reengineering of current communication services. In spite of this continuing upward trend in demand, DISA has delivered transport services at an overall cost decrease to mission partners, as shown in the subsequent chart:



The previous chart compares the bandwidth delivery, including multiprotocol label switching (MPLS) connections, with transport costs. Since FY 2015, DISA has increased transport bandwidth delivery capacity 157.6 percent to meet customer demand. The increase is driven by internet traffic, DoD Enterprise Services, full motion video collaboration, and intelligence, surveillance, and reconnaissance (ISR) requirements. Over the same timeframe, transport costs associated with the physical connections between sites have decreased by 5.7 percent. Additionally, DISA has been able to keep these costs down without any degradation in service. The DISN continues to meet or exceed network performance goals for circuit availability and latency, two key performance metrics.

The DISN has operating metrics tied to the department's strategic goal of information dominance. These operational metrics include the cycle time for delivery of data and satellite services as well as service performance objectives such as availability, quality of service, and security measures. Additionally, the IT Enterprise Services roadmap sets a DISN performance target of 99.997 percent operational availability at all Joint Staff-validated locations. DISA is working to meet the intent of this guidance through the evolving Joint Information Environment architecture and by building out the network as necessary to provide a growing number of enterprise services. These categories of metrics have guided the development of the Telecommunication Services budget submission. Shown below are major performance and performance improvement measures:

Figure 2- Major Performance and Performance Improvement Measures

SERVICE OBJECTIVE	FY 2020 Estimated Actual	FY 2021 Operational Goal	FY 2022 Operational Goal
Non-Secure Internet Protocol Router Network access circuit availability	99.77%	98.50%	98.50%
Secure Internet Protocol Router Network latency (measurement of network delay) in the continental United States	45.43 Milliseconds (CONUS INTRA)	<= 100 milliseconds	<= 100 milliseconds
Optical Transport network availability	99.63%	99.50%	99.50%

Enterprise Acquisition Services Performance Measures

The EAS business area is the department's ideal source for procurement of best-value and commercially competitive IT. EAS provides contracting services for IT and telecommunications acquisitions from the commercial sector and contracting support to the DISN programs, as well as to other DISA, DoD, and authorized non-defense customers. These contracting services are provided through DISA's DITCO and include acquisition planning, procurement, tariff surveillance, cost and price analyses, and contract administration. These services provide end-to-end support for the mission partner. The following performance measures apply for EAS:

Figure 3-EAS Performance Measures

SERVICE OBJECTIVE	FY 2020 Estimated Actual	FY 2021 Operational Goal*	FY 2022 Operational Goal*
Percent of total eligible contract dollars completed	76.4%	73.00%	73.00%
Percent of total eligible contract dollars awarded to small businesses	24.00%	28.00%	28.00%

*FY 2021 and FY 2022 goals for percent of total eligible contract dollars competed are estimates based on the released FY 2020 goal. Defense Pricing and Contract (DPC) or Industrial Policy (IP) has not yet released the goals.

In addition to the program performance measures outlined above, DISA has increased accountability of its assets by linking performance standards to internal control standards. Each Senior Executive Service member at DISA has included in their performance appraisal a standard to achieve accountability of property. This standard has filtered down to many of the managers across the agency. This increased focus on accountability has had a significant impact on the focus these leaders have in the critical area of safeguarding assets.

3. Analysis of Entity's Financial Statements

Background

DISA prepares annual financial statements in conformity with accounting principles generally accepted in the United States. The accompanying financial statements and footnotes are prepared in accordance with Office of Management and Budget (OMB) Circular A-136, *Financial Reporting Requirements.* DISA records accounting transactions on both an accrual and budgetary basis of accounting. Under the accrual method, revenue is recognized when earned and costs/expenses are recognized when incurred, without regard to receipt or payment of cash. Budgetary accounting facilitates compliance with legal constraints and controls over the use of federal funds

Since FY 2005, DISA has had an established audit committee to oversee progress towards financial management reform and audit readiness. DISA leadership participates in audit committee meetings to fully support the audit and maintain senior leader tone-at-the-top. The DISA Audit Committee is composed of three members who are not part of DISA. The current mission of the DISA Audit Committee is to serve in an advisory role to DISA senior managers. The committee is tasked with developing, raising, and resolving matters of financial compliance and internal controls with the purpose of ensuring DISA's consistent demonstration of accurate and supportable financial reports. The committee develops and enforces guidance established for this purpose.

DISA WCF did not use a significant amount of its current year budgetary resources to prevent, prepare for, or respond to COVID-19.

Defense Working Capital Fund Financial Highlights

The following section provides an executive summary and brief description of the nature of each WCF financial statement, significant fluctuations, and significant balances to help clarify their link to DISA operations.

Executive Summary

The DISA WCF Footnote 3 Status of Fund Balance with the U.S. Department of the Treasury (Line 1.A Unobligated Balance Available) reflects the results of budget execution that saw the fund decrease $256.4 million for a total of $98.4 million on its unobligated balance available, as compared with the fourth quarter of FY 2020.

- The Statement of Net Cost reflects a loss through the fourth quarter of FY 2021 of $278.2 million and includes the non-recoverable depreciation expense for network equipment transferred to DISA WCF (TSEAS PE55).

- Obligations incurred decreased by $36.6 million, in comparison with the fourth quarter of last year.

- Cash levels remained positive through the fourth quarter of FY 2021 at 11.6 days of operating cash.

- Beginning in FY 2020, DISA WCF began budgeting and executing as a "one-fund" entity. For reflecting the one-fund execution within the Defense Departmental Reporting System-Budgetary

(DDRS-B) as well as the Defense Departmental Reporting System-Audited Financial Statements (DDRS-AFS), the intra-DISA WCF business (CS-TSEAS) is removed from the DDRS-B statements/trial balances prior to going final and imported into AFS.

- The following financial statement presents an explanation of amounts reported in significant financial statement line items and/or financial notes, and variances between the fourth quarter of FY 2021 reported balances and the fourth quarter of FY 2020. Balances that have the same underlying explanation between budgetary and proprietary accounts are explained from the proprietary perspective and referenced from the budgetary perspective. Due to rounding, tables in this document may not add to overall totals.

STATEMENT OF NET COST

The Statement of Net Cost presents the cost of operating DISA programs. The goal of the revolving fund is to break even over the long term as identified in the budget, thus driving toward an objective where a profit or loss is not a target over time, but rather nets to zero.

- *Net Cost of Operations* – Net Cost of Operations decreased $164.6 million (37 percent) between the fourth quarter of FY 2020 and the fourth quarter of FY 2021 primarily due to the increase in earned revenue of $477.9 million being greater than the increase in gross cost of $313.3 million between fiscal years.

Figure 4- Net Cost of Operations

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS	$ 122,556	$ 122,252	$ 304	0%
TSEAS	155,638	322,622	(166,984)	-52%
Component	-	(2,082)	2,082	0%
Total	$ 278,194	$ 442,792	$ (164,598)	-37%

WCF Net Cost of Operations includes non-recoverable costs such as depreciation expense and imputed costs.

Gross Cost - Gross Cost totaling $8.4 billion increased $313.3 million (4 percent) between the fourth quarter of FY 2020 and the fourth quarter of FY 2021. In accordance with regulations and guidance, this reflects the full cost of the DISA WCF to include recoverable and non-recoverable costs. The primary drivers contributing to the net increase in gross costs are highlighted in the following table:

Figure 5- Gross Cost

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
Total Gross Cost	$8,383,736	$8,070,483	$ 313,253	4%
Less: PE56 Cost	5,786,284	5,700,534	85,750	2%
Less: Non-Recoverable Depreciation	171,977	189,565	(17,589)	-9%
Total DISA WCF Operating Cost	$2,425,475	$2,180,384	$ 245,092	11%
TSEAS (PE55)				
Transport Services	$ 498,209	$ 546,659	$ (48,451)	-9%
Delivery Services	163,487	163,431	56	0%
Fourth Estate Network Optimization	77,370	68,062	9,308	14%
Department of Defense 365 (DoD365)	22,900	-	22,900	100%
Cybersecurity Activities	299,027	274,104	24,923	9%
Reimbursable Telecommunications Services	$ 890,296	$ 840,746	$ 49,550	6%
CS (PE54)				
Rate Based Server/Storage Infrastructure	$ -	$ 113,311	$ (113,311)	-100%
Reimbursable Pass Through Unisys	28,561	53,374	(24,814)	-46%
Mainframe				
Rate Based Server Storage	50,869	49,886	983	2%
Reimbursable Pass Through Server Dedicated	85,673	77,233	8,440	11%
Converged Hardware				
Rate Based IBM Mainframe	87,758	74,225	13,533	18%
Imputed Cost Adjustment	31,982	-	31,982	100%
Milcloud 2.0 Migration Services	54,301	-	54,301	100%
Rate Based Server Basic	141,697	-	141,697	100%
Costs for Remaining Programs	$ (6,654)	$ (80,649)	$ 73,995	-92%

*Additional programs added to explain the FY 2021 to FY2020 variance which changes the cost for remaining programs

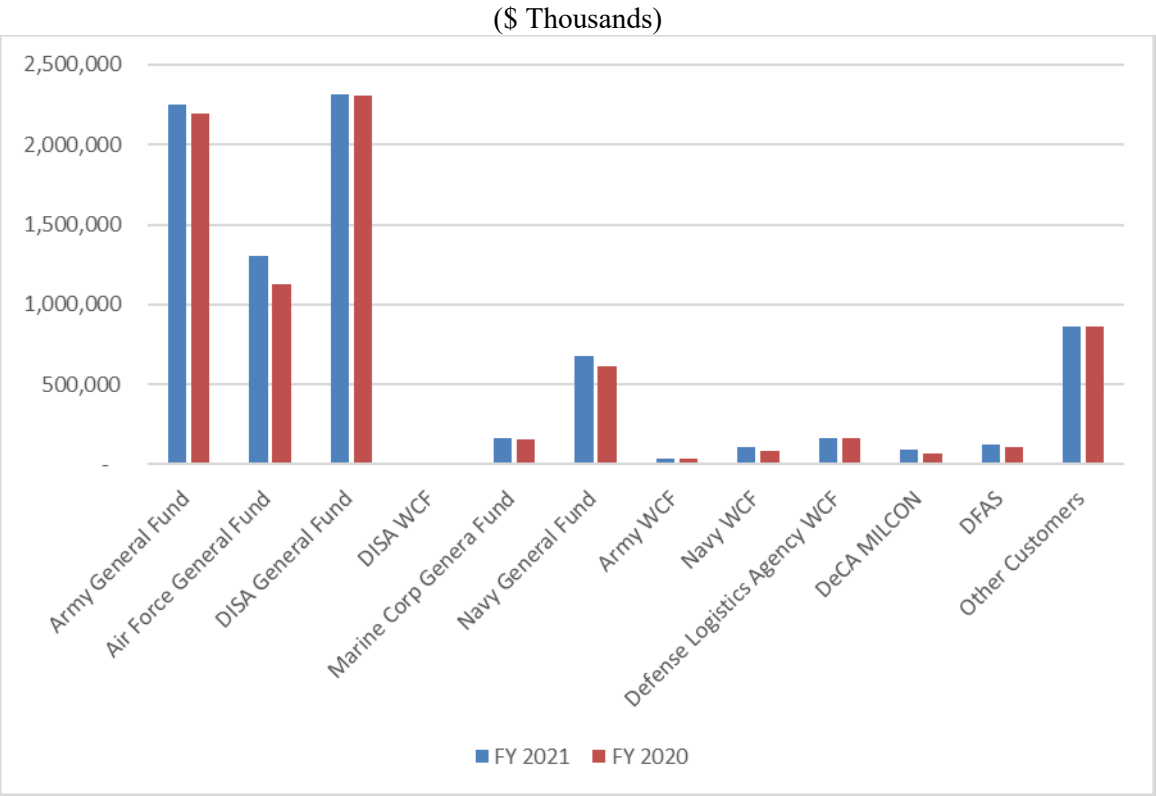
- Non-Recoverable depreciation decreased $17.6 million between fiscal years. This decrease is a result of less transfer-in of general property, plant, and equipment along with associated non-recoverable depreciation from the DISA General Fund (GF) without reimbursement in FY 2021.

Earned Revenue - Earned Revenue totaling $8.1 billion increased $477.9 million (6 percent) between the fourth quarter of FY 2020 and the fourth quarter of FY 2021.

- The Army, DISA GF, and Air Force continue to be DISA WCF's biggest customers.

The bar chart below reflects earned revenue per customer for FY 2021 and FY 2020.

Figure 6- Earned Revenue by Customer



Net Cost of Operations - Some major drivers of the change in net cost of operations between fiscal years include the following:

- CS (PE54) net cost increased between fiscal years in the Rate Based Server/Storage Infrastructure for $26.2 million.
- CS (PE54) net cost increased between fiscal years in the Rate Based IBM Mainframe Processing for $16.5 million.
- CS (PE54) net cost decreased between fiscal years in the Rate Based Floor Space Rental for $15.3 million.
- CS (PE54) net cost decreased between fiscal years in the Rate Based milCloud 2.0 Migration Services for $12.5 million.
- TSEAS (PE55) Reimbursable Telecommunication Services net cost increased $27.6 million between fiscal years.
- TSEAS (PE55) Cybersecurity Activities net cost increased $24.9 million between fiscal years.
- TSEAS (PE55) DISN Infrastructure Services Revenue net cost decreased $190.1 million between fiscal years.
- TSEAS (PE55) Transport Services net cost decreased $54.1 million between fiscal years.

BALANCE SHEET

The balance sheet presents amounts available for use by DISA (assets) against amounts owed (liabilities) and amounts that comprise the difference (net position).

Assets

Total assets of $2 billion comprise primarily Fund Balance with Treasury ($213.7 million), Intragovernmental Accounts Receivable ($894.4 million), and General Property, Plant, and Equipment (PP&E) ($908.3 million).

Figure 7- Fund Balance with Treasury

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS Beginning Balance	$ 130,876	$ 267,695	$ (136,819)	-51%
CS YTD	547,418	(136,819)	684,237	-500%
CS Total	$ 678,294	$ 130,876	$ 547,418	418%
TS Beginning Balance	$ 66,646	$ 284,850	$ (218,204)	-77%
TS YTD	(531,287)	(218,204)	(313,083)	143%
TS Total	$ (464,641)	$ 66,646	$ (531,287)	-797%
Total Beginning Balance	$ 197,522	$ 552,545	$ (355,023)	-64%
YTD	16,131	(355,023)	371,154	-105%
Total ITD Balance	$ 213,653	$ 197,522	$ 16,131	8%

Fund Balance with Treasury - Fund Balance with Treasury Inception to Date (ITD) Balance increased $16.1 million (8 percent) over last year. The following chart displays fiscal year to date (FYTD) net cash flow from current year operations (collections less disbursements) reported to Treasury for FY 2021 and FY 2020, as reflected in the monthly AR(M) 1307 Cash Flow report, presented in a comparative manner:

- The $213.7 million cash balance at Sept. 30, 2021, comprises a $197.5 million current year beginning balance and a FYTD $16.1 million increase from current year operations (includes capital outlays).
- The $16.1 million increase is $141 million more than the $124.9 million forecasted decrease in cash as reflected in the FY 2020 BES dated February 2020, with actual disbursements being $532.7 million under plan and collections being $391.7 million under plan.
- The CS current year increase in cash from operations of $547.4 million is $556.9 million more than the planned decrease of $9.4 million. The increase in cash is in line with the decrease in accounts receivable.
- The TSEAS current year decrease in cash from operations of $531.3 million is $415.8 million less than the planned decrease of $115.4 million with a contributing factor being the decrease in accounts receivable between fiscal years.
- The $213.7 million WCF ITD cash balance represents approximately 11.6 days of cash on hand ($213.7/$18.4M).

- Amounts recorded in the general ledger for Fund Balance with Treasury (FBWT) have been 100 percent reconciled to amounts reported in the DFAS Cash Management Report (CMR), representing DISA WCF's portion of the TI97 .005 account balances reported by Department of Treasury. All reconciling differences (i.e., undistributed) have been identified at the voucher level.
- The DISA WCF ITD FBWT balance remains a key figure in evaluating the "health" of the fund.

Accounts Receivable, Net - Accounts Receivable decreased $70.4 million (7 percent). The largest decrease is within the TSEAS intragovernmental receivables. Decrease is in EAS (PE56), Contracting and Acquisition Support and IT Contracts. This is offset by increases in Telecommunications Services (PE55), Security and Compliance Services, and Transport Services as well as in EAS (PE56), Enterprise License Agreements.

The table below compares current year with prior year intragovernmental and public receivable balances.

Figure 8-Accounts Receivable, Net

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS				
Intragov.	$ 98,664	$ 74,351	$ 24,313	33%
Public	112	84	28	33%
TSEAS				
Intragov.	893,440	988,394	(94,954)	-10%
Public	878	1,512	(634)	-42%
Component				
Intragov.	(97,700)	(98,584)	884	-1%
Public	-	-	-	0%
Total				
Intragov.	894,404	964,161	(69,757)	-7%
Public	989	1,596	(606)	-38%
Total	$ 895,393	$ 965,757	$ (70,363)	-7%

General Property, Plant, and Equipment, Net – DISA WCF general PP&E consists primarily of equipment used by DISA organizations to deliver computing services to customers in the DISA Computing Ecosystem and telecommunication services over the DISN.

Figure 9-General PP&E, Net

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS	$ 211,417	$ 219,521	$ (8,104)	-4%
TSEAS	696,871	671,083	25,789	4%
Total	$ 908,288	$ 890,604	$ 17,684	2%

- PP&E increased $17.7 million (2 percent) and includes capital assets funded by DISA WCF operations, capital assets supporting the infrastructure of the services offered by the WCF that are transferred in from the DISA GF without reimbursement, as well as current period depreciation expense on existing assets. The depreciation expense associated with these capital assets is non-recoverable.

- Non-recoverable depreciation expenses decreased $17.6 million between fiscal years. This decrease is a result of less transfer-in of general property, plant, and equipment along with associated non-recoverable depreciation from the DISA GF without reimbursement in FY 2021.

Over 70 percent of the WCF PP&E balances are composed of the following categories:

Figure 10- PP&E-Net Book Value

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
WCF NBV	$908,288	$ 890,604	$ 17,684	
CS PP&E	211,417	219,521	(8,104)	23%
Joint Regional Security Stacks	188,575	196,503	(7,927)	21%
Multiprotocol Label Switching	58,221	89,472	(31,251)	6%
Optical Transport Network	64,754	69,601	(4,846)	7%
TSEAS DPAS Values	84,573	38,586	45,988	9%
Fiber IRUs	30,895	41,266	(10,370)	3%
TSEAS Assets Pending	119,988	71,077	48,911	13%
Subtotal	$ 758,424	$ 726,024	$ 32,400	84%
Non-Recoverable Depreciation	171,977	189,565	(17,589)	19%
Total	$ 930,401	$ 915,589	$ 14,811	102%

Other Assets - Advances and prepayments decreased $841 thousand (100 percent) within TSEAS as the result of an adjustment to reconcile trading partner data.

Other Assets balances as of Sept. 30, 2021, and Sept. 30, 2020, are as follows:

Figure 11-Other Assets

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS				
Intragov.	-	-	-	0%
Public	-	-	-	0%
TSEAS				
Intragov.	-	841	(841)	-100%
Public	-	-	-	0%
Total	$ -	$ 841	$ (841)	-100%

Liabilities

Total liabilities of $1 billion comprised primarily intragovernmental accounts payable ($23.9 million), intragovernmental other liabilities ($5.9 million), non-federal accounts payable ($950.5 million), other federal employment benefits ($6 million), and non-federal other liabilities ($57.5 million).

Total Liabilities Not Covered by Budgetary Resources - Total liabilities not covered by budgetary resources increased $239 thousand (4 percent) and is composed of other liabilities, military retirement benefits and the unfunded federal employees' compensation act (FECA) liability.

Figure 12-Total Liabilities Not Covered by Budgetary Resources

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS	3,207	3,064	143	5%
TSEAS	2,466	2,370	96	4%
Total	$ 5,673	$ 5,434	$ 239	4%

Liabilities Covered by Budgetary Resources - Liabilities covered by budgetary resources increased $44.7 million (5 percent). The largest portion of the balance is made up of EAS IT contracts. The table below compares current year with prior year liabilities covered by budgetary resources and includes the public accounts payable balances.

Figure 13-Total Liabilities Covered by Budgetary Resources

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS	$ 131,155	$ 135,005	$ (3,850)	-3%
TSEAS	1,004,695	956,985	47,710	5%
Component	(97,700)	(98,584)	884	-1%
Total	$ 1,038,149	$ 993,406	$ 44,744	5%

From a customer funding perspective, the DISA GF and Army continue to provide the most customer-funded contract requirements associated with the public accounts payable balance. The increase in accounts payable is primarily attributed to increases in EAS, IT Contracts, offset by a decrease in Telecommunication Contracts. The decrease in PE54 is due to capacity services decreasing.

Other Liabilities - Other Liabilities increased $6.3 million (11 percent) primarily driven by the increase in accrued funded payroll and benefits for $6.7 million.

Figure 14-Other Liabilities

(in thousands)

	9/30/2021	9/30/2020	Inc/Dec	% Chg.
CS				
Intragovernmental	$ 3,300	$ 2,791	$ 509	18%
Public	31,162	26,568	4,594	17%
TS				
Intragovernmental	2,632	1,945	687	35%
Public	26,379	25,918	461	2%
Total				
Intragovernmental	5,932	4,736	1,196	25%
Public	57,541	52,486	5,055	10%
Total Other Liabilities	$ 63,473	$ 57,222	$ 6,251	11%

STATEMENT OF CHANGES IN NET POSITION

The Statement of Changes in Net Position presents the change in net position during the reporting period. The DISA WCF net position is affected by changes to its two components, other financing sources (transfers in/out without reimbursement and imputed financing from costs absorbed by others), and Net Cost of Operations (Cumulative Results of Operations).

- Transfers in/out without reimbursement decreased $103.9 million (47 percent) primarily in Telecommunication Services, specifically Transport Services. This decrease is a result of less transfer-in of general property, plant, and equipment along with associated non-recoverable depreciation from the DISA GF without reimbursement in FY 2021.
- Imputed financing costs absorbed by others increased $1.1 million (2 percent) due to an increase in imputed cost related to employee benefits.
- Net Cost of Operations decreased $164.6 million (37 percent) as discussed in the Statement of Net Cost section.

STATEMENT OF BUDGETARY RESOURCES

The Statement of Budgetary Resources (SBR) provides information about how budgetary resources were made available and their status at the end of the period. It is the only financial statement derived entirely from the budgetary USSGL accounts, and is presented in a combined, not consolidated basis to remain consistent with the SF133, Report on Budget Execution and Budgetary Resources.

Figure 15-Statement of Budgetary Resources

(in thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
CS				
Obligations Incurred	$ 332,733	$ 1,061,129	$ (728,396)	-69%
Unobligated Balances	677,228	75,997	601,231	791%
Contract Authority	25,995	47,772	(21,777)	-46%
Unfilled Customer Orders	100,634	97,832	2,802	3%
TSEAS				
Obligations Incurred	7,681,802	7,834,248	(152,445)	-2%
Unobligated Balances	(549,105)	273,290	(822,395)	-301%
Contract Authority	109,324	185,178	(75,855)	-41%
Unfilled Customer Orders	2,685,911	2,953,884	(267,973)	-9%
Component				
Obligations Incurred	(1,154,647)	(1,081,410)	(73,236)	7%
Unobligated Balances	(29,759)	5,431	(35,189)	-648%
Contract Authority	-	-	-	0%
Unfilled Customer Orders	(2,062,895)	(976,983)	(1,085,912)	111%
Total				
Obligations Incurred	6,859,888	7,813,967	(954,079)	-12%
Unobligated Balances	98,364	354,718	(256,354)	-72%
Contract Authority	135,319	232,950	(97,631)	-42%
Unfilled Customer Orders	$ 723,650	$ 2,074,733	$(1,351,083)	-65%

New Obligations and Upward Adjustments (line 2190) - Obligations incurred decreased $993.1 million (50 percent). In the following chart, total obligations incurred FYTD are sourced from and agree with the DDRS AFS statements for both TSEAS and CS. Program-level detail are sourced from the Financial Accounting and Management Information System (FAMIS) WCF for TSEAS and BERT for CS. The major drivers for obligations incurred for the DISA WCF are as follows:

Figure 16-Obligations Incurred

(thousands)

	9/30/2021	9/30/2020	Inc./(Dec.)	% Chg.
Total Obligations Incurred	$ 6,859,888	$ 7,813,966	$ (954,078)	-12%
Less: PE56 Obligations Incurred	5,777,302	5,790,118	(12,816)	0%
Less: PE56 On The Top Adjustments	96,021	(114,706)	210,727	-184%
Total DISA WCF Funded Obligations	(986,565)	2,138,554	(1,151,989)	-54%
TSEAS (PE55)				
Adjustment to remove the budgetary impact of Intra DISA WCF collections and disbursements	(148,964)	-	(148,964)	-100%
Contracting and Acquisition Support	(136)	27,678	(27,814)	-100%
Core Sustaining Activities	97,375	114,423	(17,047)	-15%
Maintenance	100,275	109,584	(9,308)	-8%
Network Support Services	26,886	23,809	3,077	13%
Comsat Fixed Satellite Services	627,868	582,426	45,442	8%
CS (PE54)				
Adjustment to remove the budgetary impact of Intra DISA WCF collections and disbursements	(795,549)	-	(795,549)	-100%
Server Dedicated Converged Hardware	-	70,147	(70,147)	-100%
Unisys Mainframe	18,817	33,964	(15,147)	-45%
Rate Based Global Content Delivery Service	35,736	38,201	(2,465)	-6%
Rate Based Server Storage	40,029	34,891	5,138	15%
Component (DISA99)				
Intra-WCF One Fund Adjustment	(1,154,234)	(1,081,410)	(72,824)	7%
All Other Programs Balances	$ 2,138,462	$ 2,184,843	$ (46,381)	-2%

- Largest decrease for Component (DISA99) was due to removing the Intra-DISA WCF business from DDRS-B.
- DISA WCF incorporated a top-sided adjustment for TSEAS accounts payable/expense and accounts receivable/revenue that affected the obligations incurred for the prior FY. This was done in FY21 to report corrected comparative numbers.
- Largest decrease for TSEAS (PE55) was in the DISN Reimbursable Services business line, specifically Comsat Fixed Satellite Services as well as an adjustment done to remove the budgetary impact of intra DISA WCF collections and disbursements.
- Largest decreases for CS (PE54) were in Reimbursable Pass-Through Server Dedicated Converged Hardware as well as an adjustment done to remove the budgetary impact of intra DISA WCF collections and disbursements.

Unobligated Balance, End of Period (line 2490) - The unobligated balance as of Sept. 30, 2021, decreased $256.4 million (72 percent) between fiscal years and is primarily at the Component level and was due to adjusting the Intra-DISA WCF Business for DDRS-B as well as more obligations incurred compared with orders received within CS and TSEAS, specifically in Enterprise License Agreements.

Unobligated Balance, End of Period reflects the remaining balance in the following accounts at the end of the period; Apportionments – Anticipated Resources (USSGL 4590), Allotments – Realized (USSGL 4610), and Commitments – Subject to Apportionment (USSGL 4700).

Contract Authority (line 1690) - Contract authority decreased $97.6 million (42 percent) between fiscal years due to the requirement that collections for $85.3 million in budgeted depreciation were applied to unliquidated contract authority and were not used as additional operating authority.

Unfilled Customer Orders (USSGL 4221) - Unfilled customer orders decreased $1.4 billion (65 percent) between fiscal years is primarily at the Component level and was due to removing the Intra-DISA WCF Business from DDRS-B. The remaining decrease in TSEAS is attributed to in EAS IT Contracts as well as Enterprise License Agreements.

Outlays, Net (Line 4190) **-** Decreased $353.9 million (105 percent) between fiscal years primarily due to an adjustment to remove the budgetary impact of intra DISA WCF collections and disbursements. This line is reported as negative in this fiscal year due to collections being higher than disbursements. The offsetting increase is primarily in EAS, specifically Enterprise License Agreements.

In order to report as one fund, the budgetary collections (USSGL 4252) and outlays (USSGL 4902) were removed from the associated lines, 1890 and 2190 on the Statement of Budgetary Resources.

RECONCILIATION OF NET COST TO NET OUTLAYS

The purpose of the reconciliation of Net Costs to Outlays is to explain how budgetary resources applied during the period relate to the net cost of operations for the reporting entity. This information is presented in a way that clarifies the relationship between the outlays reported through budgetary accounting and the accrual basis of financial (i.e., proprietary) accounting. By explaining this relationship, the reconciliation provides the information necessary to understand how the budgetary outlays finance the net cost of operations and affect the assets and liabilities of the reporting entity. Most variances on this note are addressed in other sections above, but those not explained will be provided as required.

4. Management Discussion and Analysis of Systems, Controls, and Legal Compliance

Management Assurances

DISA's management structure, policies and procedures, and internal control reviews of key mission processes contribute to the assurance that our internal controls are operating as intended. Our governance board and internal control structure, along with the Risk Management and Internal Control (RMIC) Program is managed through a three-tiered approach, as described in subsequent paragraphs. The first tier is supported by the DISA Senior Assessment Team (SAT), which provides guidance and oversight to the RMIC Program. The second tier is supported by the subject matter expert internal control (IC) team, and the third tier is supported by the assessable unit managers (AUMs) who manage at the program/directorate level within the organization. The SAT and IC teams maintain a charter that is available on DISA's webpage. AUMs are appointed in writing each year, and the appointment letter delineates the role and responsibilities of the AUMs.

DISA delegates authority only to the extent required to achieve objectives, and management evaluates the delegation for proper segregation of duties to prevent fraud, waste, and abuse. In addition, DISA relies on external stakeholders, such as the DFAS as our accounting data processor, bill payer, and payroll processor, to better achieve our mission as documented in an SLA.

The DISA Office of the Inspector General (OIG) maintains a hotline for the anonymous reporting of ethics and integrity issues that is available to employees 24 hours a day, seven days a week. Additionally, DISA OIG conducts reviews and inspections to identify or prevent instances of fraud, waste, and abuse.

The Office of the Chief Financial Officer (OCFO)/Comptroller has oversight of DISA's RMIC Program. Agency AUMs perform testing and report results for Internal Controls Over Reporting - Operations (ICOR-O) Non-Financial. Tests and reports of results are conducted for the Internal Controls Over Reporting - Financial Systems (ICOR-FS) for the agency. In addition, the OCFO Office conducts testing and reports on the overall Internal Controls Over Reporting - Financial Reporting (ICOR-FR) for the agency.

Testing is conducted to ensure the internal control structure is adhering to the components of the Government Accountability Office (GAO) Green Book objectives of operations, reporting, and compliance. DISA's senior management evaluated the system of internal control in effect during the fiscal year as of the date of this memorandum, according to the guidance in the OMB Circular No. A-123 and the GAO Green Book. Included is our evaluation of whether the system of internal controls for DISA is compliant with standards prescribed by the comptroller general.

The objectives of the system of internal controls are to provide reasonable assurance for

- Operations: effectiveness and efficiency of operations.
- Reporting: reliability of financial and non-financial reporting for internal and external use.
- Compliance: adherence to applicable laws and regulations, including financial information systems compliance with the Federal Financial Management Improvement Act (FFMIA) of 1996 (Public Law 104-208).

The evaluation of internal controls extends to every responsibility and activity undertaken by DISA and applies to program, administrative, and operational controls. Furthermore, the concept of reasonable assurance recognizes that DISA's mission objectives are achieved and that

1. the cost of internal controls should not exceed the benefits expected to be derived.
2. the benefits include reducing the risk associated while achieving the stated objectives.

Moreover, errors or irregularities may occur and not be detected because of inherent limitations in any system of internal controls, including those limitations resulting from resource constraints, congressional restrictions, and other factors. Finally, projection of any system evaluation to future periods is subject to the risk that procedures may be inadequate because of changes in conditions, or that the degree of compliance with procedures may deteriorate. Therefore, this statement of reasonable assurance is provided within the limits of the preceding description.

DISA management evaluated the system of internal controls in accordance with the guidelines identified above. The results indicate that the system of internal controls of DISA, in effect as of the date of this memorandum, taken as a whole, complies with the requirement to provide reasonable assurance that the above-mentioned objectives were achieved for operations and compliance. Due to the inconsistencies surrounding reporting, reasonable assurance has not been achieved, primarily because of the exceptions identified on DISA's GF. This position on reasonable assurance is within the limits described in the preceding paragraph.

FY21 Internal Control Program Initiatives and Execution

In FY 2020, the Manager's Internal Control Program (MICP) was renamed to the RMIC Program. In FY2021, there were requirements with a focus on the priorities of correcting prior year significant deficiencies and material weaknesses (MW); entity level controls; risk assessments aligned to performance management and key processes; oversight and monitoring; Coronavirus Aid, Relief, and Economic Security (CARES) Act Spending compliance; fraud control leading practices; improper payment recovery; and Security Assistance Accounts. In executing DISA's internal control program, each of these areas are highlighted below.

A. Correction of Prior Year Significant Deficiencies and Material Weaknesses

One of the department's focus areas is to make progress towards resolution of prior year MWs and conditions impeding audit progress. DISA has made concentrated efforts to resolve and clear prior year issues. In FY 2021, DISA remedied and submitted requests for closure of 47 validated corrective action plans. At the time of this memorandum, five have been approved for closure by the independent audit firm (IPA).

B. Entity Level Controls (ELCs)

ELCs represent the overriding management controls that create an environment of management oversight for the financial and non-financial activities of the department and DISA as an agency. DISA management develops and maintains internal control activities that comply with the five standards promulgated by the GAO. These include Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. Underlying these five control components, the Green Book states 17 control principles that represent fundamental elements associated with each component of control and recognizing that there are significant interdependencies among the various control principles. As a focal point in the FY 2021 audit, DISA's IPA was briefed on 15 walkthroughs that provided an overview as well as discussions of the controls in place.

C. Enterprise Approach to Risk Management

Through its risk assessment, DISA has taken an enterprise approach that covers key business processes. Risk management has been aligned to the National Defense Strategy (NDS) and the National Defense Business Operations Plan (NDBOP). DISA supported NDS Strategic Goal 3 to "Reform the Department's Business Practices for Greater Performance and Affordability" through identifying associated control activities and evaluating risk and control effectiveness. In addition, DISA adheres to the NDBOP goal to "undergo an audit and improve the quality of budgetary and financial information that is most valuable in

managing the DoD," through its audit and continuous environment of improvement and refining processes. The RMIC Program is managed through a three-tiered approach, which provides a structure to identify risk at an enterprise level, as well as at a more granular level. The DISA director provides a "tone-at-the-top" memo that defines management's leadership and commitment towards an effective internal control structure. The second tier is supported by the Internal Control team, consisting of subject matter experts providing guidance and execution of the program throughout the agency. The third tier is supported by the AUMs who manage at the program/directorate level within the organization. Each directorate's senior leadership, in coordination with each assessable unit, identify areas of risks, based upon collaboration with their respective area. The coordination and consolidation of risk identifies the overall assessment of risk at the enterprise risk management level, while also reviewing DISA's detail transactions.

D. Oversight and Monitoring

DISA's internal control structure of training provides assistance to AUMs; ELCs; risk assessments; continuous testing in mandatory and high-risk areas; reviews, updates and management approval of process narratives and cycle-memos; corrective action plans (CAPs); and senior accountable officials (SOAs) letters of assurance are all core to an integral program of oversight and monitoring. In addition, the SAT met on Aug. 5, 2021, and provided oversight to the internal control program through discussion of results and anticipated outcomes to be reported in the FY 2021 Statement of Assurance.

E. Payment Integrity/Improper Payment Recovery

For compliance with the Payment Integrity Information Act of 2019 (Pub. L. No. 116-117, 31 U.S.C. § 3352 and § 3357), DISA has an internal control structure in place to mitigate improper payments that could result in payment recovery actions. Actions taken to prevent overpayments include testing and review of civilian time and attendance, travel payments, and purchase card transactions. Tests validate that internal controls are in place and functioning as preventative measures to mitigate risks in the execution, obligation and liquidation of funding for transactions. Controls are in place through established policy and procedures, training, separation of duties and data mining to identify risks and fraud vulnerabilities. Additionally, the DFAS, as DISA's accounting service provider, performs overpayment recapture functions on behalf of DISA. DFAS includes DISA transactions in their sampling populations for improper payment testing. There have been no reportable issues regarding payment integrity and improper payment recovery in FY 2021.

F. CARES Act/COVID-19

The Department of Defense was allocated $10 billion in the CARES Act signed on March 2, 2020, (Public Law 116-136), to support military response to the public health emergency domestically and internationally. DISA has been allotted $182.9 million in CARES Act funding. The CARES Act provides the DoD flexibility in executing contract actions to expedite disbursement of these funds efficiently and effectively. In execution of this funding, the risk for fraud, waste, and abuse is heightened when internal controls are relaxed. COVID19-related activity has been reviewed and tested using verification and validation (V&V) procedures. There have been no laws compromised or major issues identified leading to fraud, waste or abuse as validated through testing results for FY 2021. Areas of improvements for CARES Act execution include ensuring requirements are aligned with spending plans and ensuring that transactions accurately reflect the Disaster Emergency Fund Code (DEFC) and National Interest Action (NIA) code.

G. Fraud Controls

In FY 2021, the DISA fraud control environment was evaluated by using the DoD Fraud Control Assessment template. The template includes example of control attributes related to the GAO leading practices to assist with identifying existing fraud controls and identifying gaps that require designing new

or additional controls. The GAO framework includes 11 leading practices that were considered for ICOR-O, ICOR-FR, and ICOR-FS for high-risk focus areas.

H. Security Assistance Agency (SAA)/Foreign Military Sales (FMS)

DISA is an implementing agency (IA) that supports the execution of military assistance programs. The IA is responsible for the overall management of the actions that will result in delivery of the materials or services as stated in agreements established between a foreign country or international organization and DISA. In partnership with the Defense Security Cooperation Agency (DSCA), DISA is in the initial stages of a financial statement audit. As of this fiscal year, DISA does not have a financial reporting function in place to warrant an audit. However, the internal control structure already in place for DISA's GF and WCF is leveraged for the FMS process. FMS is under the umbrella of the Development and Business Center (DBC), which performs mandatory operational testing and is included in the organization's letter of assurance.

I. Data Act Data Quality Testing

The OMB published memorandum 18-16, *Appendix A to OMB Circular A-123, Management of Reporting and Data Integrity Risk*, dated June 6, 2018, that outlines guidance for agencies to develop a Data Quality Plan (DQP) to achieve the objectives of the Data Accountability and Transparency Act (DATA). DISA has established a DQP that provides an emphasis on a structure for data quality on financial data elements, procurement data reporting, data standardization, and data reporting. In FY 2021, the internal control program further refined its data quality testing to review data integrity. Results of the testing provided no major issues with the established attributes in the first three quarters of the current fiscal year.

J. Accomplishments

DISA strives to improve in its internal control environment. Two significant accomplishments for financial reporting:

- Internal controls: The One Fund program consolidates the two existing DISA WCF entities into a single fund and operating environment. This environment has been successful in reporting as One Fund entity.

- Audit opinion progress: In FY 2021, the DISA WCF received an unmodified opinion on its FY 2020 financial statements. This is a tremendous accomplishment for not only DISA, but also the DoD. An achievement like this is no easy task. The numbers speak for themselves on the level of effort needed to support the audit. For the WCF, there were 854 provided by client (PBC) requests, over 3,500 samples with over 13,000 artifacts provided. These numbers don't include the time spent in meetings and walkthroughs with the auditors and are more impressive when you take a step back and realize that during most of the year, the audit work was done virtually due to the COVID-19 pandemic.

Internal Control Structure

Using the following process, DISA evaluated its system of internal control and maintains a sufficient documentation/audit trail to support its evaluation and level of assurance. DISA manages the RMIC Program through a three-tiered approach. The first tier is supported by the DISA SAT, which provides guidance and oversight to the RMIC Program. In FY 2021, the DISA director signed a "tone-at-the-top" memo, which defines management's leadership and commitment towards an effective RMIC: openness,

honesty, integrity, and ethical behavior. The memo directed the agency to ensure a risk-based and results-oriented program in alignment with the GAO Green Book and OMB A-123. The tone at the top is set by all levels of management and has a trickle-down effect on all employees.
The second tier is supported by a subject matter expert (SME) team. The team coordinates requirements with the Office of the Secretary of Defense (OSD) Comptroller regarding the RMIC in addition to providing guidance, oversight, and validation in accordance with OSD Directives to the AUMs. DISA provided internal control training for the AUMs in November 2020 and conducted additional workshops in December 2020. The RMIC team compiles assessable unit (AU) submissions for the agency's Statement of Assurance, communicates OUSD requirements to leadership, facilitates information sharing between AUMs, and consolidates results.

Identification of Material Assessable Units

The third tier is supported by the AUMs, who manage at the program/directorate level within the organization. For this reporting cycle, DISA identified 12 AUs:

- Office of the Chief Financial Officer (OCFO)
- Component and Acquisition Executive (CAE)
- Development and Business Center (DBC)
- Chief of Staff (DDC)
- Inspector General (IG)
- Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN)
- Joint Service Provider (JSP)
- Operations Center (OC)
- Procurement Services Directorate (PSD)
- Risk Management Executive (RME)
- White House Communications Agency (WHCA)
- Workforce Services and Development Directorate (WSD)

Each AU is led by at least one member of the Senior Executive Service (SES) or military flag officer, and carries a distinct mission within DISA, which in turn causes the AU to have unique operational risks that require evaluation.

Identifying Key Controls

Mandatory testing for all organizations is required to identify the functions performed within their area, in addition to the required testing areas of the Defense Travel System (DTS), Time and Attendance, and PP&E, to identify the level of process documentation available and determine the associated risk of those functions. Additionally, the AUM is responsible for identifying and documenting the key controls within their AU in accordance with DoD Instruction 5010.40. The OCFO documents processes and key controls for all ICOR-FR functions through detailed cycle memoranda and narratives. Each AU documented its key processes and risk on the **Risk Assessment Template, Illustration 1**. The OCFO RMIC team advised the AUMs to test, at a minimum, those key processes that were self-identified as high risk, as well as safety, security (if applicable), and the required testing areas.

Illustration 1: Assessable Unit Manager (AUM) Risk Assessment Template (Excerpt)

National Defense Strategic Goal	National Defense Business Operations Plan	Risk Description
Strategic Goal 3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3: Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	Ineffective processes and controls to validate the location, quantity and value of capital assets puts the Agency at risk of not meeting the objective of providing cost accounting capabilities needed to reliably account for and report on the full cost of its equipment.
Strategic Goal 3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3: Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	Competing priorities and insufficient FTEs hinder our ability to sustain auditability. DISA continues to analyze the impacts of accounting data from a September 2018 implemented financial accounting system.
Strategic Goal 3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3: Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	All requirements are not communicated and are therefore not in included in the POM.
Strategic Goal 3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3: Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	Programs would not be resourced and compliant with the Department of Defense (DoD) Chief Information Officer (CIO) Capability Programming Guidance (CPG) and/or aligned to the DISA's strategic priorities
Strategic Goal 3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3: Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	Allocation of resources may not balance to Fiscal Guidance (FG)

Developing the Test Plan/Executing the Test

Each AU completed a plan to test the controls in place for each process identified to be tested. The development of the plan, shown in Illustration 2, includes consideration of the nature, extent (including sampling technique), and timing of the execution of the controls tested. Additionally, the risk magnitude (high, medium, or low), objective type, risk type, risk response, and tolerance rate are also identified. The test method (or type) is identified within the plan.

Agency:	DISA										
AU:			Org:			Dcode(s):					
Process Name:			Preparer Name:			Preparer Phone:					
Narrative Reference:			Objective Type:			Risk Type:		Risk Response:			
Control #	Internal Control Currently In Place (Control Objective)	Control Criteria	Control Type	Control Frequency	Risk (Description)	Assigned Risk (Risk Magnitude)	Tolerance Rate	Test Plan (Description)	Test Type	Frequency of Test	

This documentation format enables the AUM to execute testing and provide the results and an abbreviated analysis, shown in **Illustration 3** below.

Illustration 3: Test Results

Agency:	DISA													
AU:		Org:			Dcode(s):									
Process Name:		Preparer Name:			Preparer Phone:									
Narrative Reference:		Objective Type:			Risk Type:		Risk Response:							
Scope	Date Tested	Population	Sample Size	Summary of Test Results	Location of Testing Documentation	# of Exceptions	Exception %	Pass/Fail	Was Control Effective?	Significant Deficiency?	Material Weakness?	Elevate Material Weakness?	New Control Risk Level?	

Internal Controls Over Reporting – Operations

Mandatory testing is required for all organizations. An AUM, in coordination with senior management, identifies the functions performed within their area, in addition to the required testing areas of DTS, time and attendance, and PP&E, to identify the level of process documentation available, and determine the associated risk of those functions. In addition, Government Purchase Card and Records Management is tested by process owners, and the results of these tests are reported in each respective area's letters of assurance.

Internal Controls over Reporting - Financial Systems

As of FY 2019, the implementation of Enterprise Resource Planning (ERP) approved systems resolved compliance issues associated with the legacy systems. Some key indicators for underlying sound internal controls include that DISA consistently provides timely and reliable financial statements to OMB within 21 calendar days at the end of the first through third quarters and unaudited financial statements to OMB, GAO, and Congress by Nov. 15 each year. DISA has not reported antideficiency violations in more than a decade, and it continues to demonstrate compliance with laws and regulations.

DISA's core financial management systems routinely provide reliable and timely information for managing day-to-day operations, as well as providing information used to prepare financial statements and maintain effective internal controls. These factors are key indicators of FFMIA compliance.

Additionally, DISA provides application hosting services for the department's service providers (DFAS; DLA; Defense Contract Management Agency (DCMA); Defense Human Resource Activity (DHRA); military services, and other defense organizations). As a result, DISA is responsible for most of the IT general controls over the computing environment in which many financial, personnel, and logistics applications reside. In order for service providers and components to rely on automated controls and documentation within these applications, controls must be appropriately and effectively designed. In FY 2021, DISA embarked on two Statement on Standards for Attestation Engagement (SSAE) 18 audits and received an unmodified opinion on Automated Time and Attendance and Production System (ATAAPS) and Hosting Services. This was the second year in a row DISA received an unmodified opinion for these services.

Internal Controls Over Reporting - Financial Reporting

The OCFO documented end-to-end business processes and identified key internal control activities supporting key business processes for ICOR-FR. DISA conducted an internal risk assessment that evaluated the results of prior year audits, internal analysis of the results of financial operations, and known upcoming business events. An internal control assessment was conducted within DISA for mission-specific key processes.

Based on the results of the internal risk analysis, internal testing was conducted to evaluate the significance of potential deficiencies identified. Specific areas of testing included the following:

General Fund	Working Capital Fund	Other
• Data Quality Plan • Dormant Reviews * • Year End Obligations • Trial Balance Rollover Verification • Eliminations (Trading Partner) • Non-DISA Site Testing * • GF Revenue • GF Expense • CARES Act Testing *	• CS Trial Balance Rollover Verification • TSEAS Trial Balance Rollover Verification • TSEAS Revenue • TSEAS Expenditure	• Active Users • Departed Users • Security Awareness Training • Separation of Duties • PP&E Additions • PP&E Disposals

*Note: *Exceptions of non-compliance.*

The details of these internal control reviews and the supporting documentation are kept on file for reference.

Financial Improvement and Audit Readiness (FIAR) led department-wide discussions regarding SSAE 18s and the impact to component financial statements. DISA identified more than 240 Complementary User Entity Controls (CUECs) that had an impact on our financial statements. In addition to our continued participation in Service Provider CUEC discussions, at the time of the statement of assurance assessment, DISA is completing the process of reviewing more than 240 identified CUECs to determine our level of risk and identified control descriptions and control attributes for each. For those CUECs determined to be common across all the identified systems, testing was conducted for areas of high risk.

The following table provides a summary of DISA's approach to the FY 2021 internal control evaluation:

Summary of Management's Approach to Internal Control Evaluation

Reporting Entity/Component Name: Defense Information Systems Agency

Summary of Component Mission: To conduct Department of Defense Information Network (DODIN) operations for the joint warfighter to enable lethality across all warfighting domains in defense of our nation.

List of all Component Organizations:

- Office of the Chief Financial Officer (OCFO)
- Component and Acquisition Executive (CAE)
- Operations & Infrastructure Center (OPIC)
- Development and Business Center (DBC)
- Chief of Staff (DDC)
- Inspector General (IG)
- Joint Force Headquarters DODIN (JFHQ-DODIN)
- Joint Service Provider (JSP)
- Operations Center (OC)
- Procurement Services Directorate (PSD)
- Risk Management Executive (RME)
- Operations & Infrastructure Center (OPIC)
- White House Communications Agency (WHCA)
- Workforce Services and Development Directorate (WSD)

List of all Component material AUs related to ICOR

- Office of the Chief Financial Officer (OCFO)
- Operations Center (OC)
- Procurement Services Directorate (PSD)

Summary of Internal Control Evaluation Approach: DISA's RMIC Program is executed in accordance with applicable laws and guidance and is managed through a three-tiered approach which provides a structure to identify risk at an enterprise level as well as more granular level. It includes the DISA Director and senior management, the internal control team and AUMs who manage at the Program/Directorate level within the organization. DISA uses a top-down, as well as bottom-up approach, to execute its internal control program. Although internal controls are in place and functioning, testing results and audit findings have revealed increased financial reporting risk operating effectiveness.

Figure 17-Overall Assessment of a System of Internal Control

Internal Control Evaluation	Designed & Implemented (Yes/No)	Operating Effectively (Yes/No)
Control Environment	Yes	Yes
Risk Assessment	Yes	No
Control Activities	Yes	Yes
Information and Communication	Yes	Yes
Monitoring	Yes	Yes
Are all components above operating together in an integrated manner?	Yes	Yes

Figure 18-Overal Evaluation of a System of Internal Control

Overall Evaluation	Operating Effectively (Yes/No)
Is the overall system of internal control effective?	Yes

In addition to the Federal Managers Financial Integrity Act (FMFIA), DISA reports its compliance with the FFMIA. FFMIA requires an assessment of adherence to financial management system requirements, accounting standards, and U.S. Standard General Ledger transaction level reporting. For FY 2021, DISA is reporting overall substantial compliance. The following is a comprehensive list of laws and regulations that were assessed for compliance by DISA WCF in context of the FY 2021 audit.

Acronym	Laws and Regulations (Supplement Number)
ADA	Antideficiency Act, 31 U.S.C. 1341 and 1517, and OMB A-11, Preparation, Submission, and Execution of the Budget, Part 4 FAM 803
DCIA	Provisions Governing Claims of the U.S. Government as provided primarily in 31 U.S.C. 3711-3720E (Including the Debt Collection Improvement Act of 1996) (DCIA) FAM 809
PPA	Prompt Payment Act, 5 CFR 1315. FAM 810
CSRA	Civil Service Retirement Act FAM 813
FEHB	Federal Employees Health Benefits Act FAM 814
FECA	Federal Employees' Compensation Act FAM 816
FERS	Federal Employees' Retirement System Act of 1986 FAM 817
PAS for CEs	Pay and Allowance System for Civilian Employees as Provided Primarily in Chapters 51-59 of Title 5, U.S. Code FAM 812
CFO Act, A-136	Chief Financial Officers (CFO) Act of 1990 and OMB Circular A-136, Financial Reporting Requirements
FFMIA	Federal Financial Management Improvement Act (FFMIA) of 1996; OMB Circular A-130, Managing Federal Information as a Strategic Resource
FMFIA and A-123	Federal Managers Financial Integrity Act (FMFIA) of 1982 and OMB Circular A-123, Appendices A through D
FISMA	Federal Information Security Management Act (FISMA) of 2002
DoD FMR	DoD, Financial Management Regulation 7000.14-R
PIIA of 2019	Payment Integrity Information Act of 2019 (PIIA); OMB Memorandum M-18-20/OMB Circular A-123, Appendix C, June 2018, modified March 5, 2021

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

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER) (OUSD(C))
DEPUTY CHIEF FINANCIAL OFFICER (DFCO)

SUBJECT: Annual Statement of Assurance Required Under the Federal Managers' Financial Integrity Act (FMFIA) for Fiscal Year (FY) 2021

As director of the Defense Information Systems Agency (DISA), I recognize DISA is responsible for managing risks and maintaining effective internal control to meet the objectives of sections 2 and 4 of the Federal Managers' Financial Integrity Act (FMFIA) of 1982. DISA conducted its assessment of risk and internal control in accordance with the Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," and the Green Book, Government Accountability Office (GAO) GAO-14-704G, "Standards for Internal Control in the Federal Government." This internal review also included an evaluation of internal controls around our Security Assistance Accounts (SAA) activities leveraged by established General Fund processes. Based on the results of the assessment, DISA can provide reasonable assurance, except for two self-reported Significant Deficiencies (SDs) (Communications Service Authorizations and Records Management) in FY 2021, reported in the "Significant Deficiencies and Material Weaknesses Template," that internal controls over operations and compliance are operating effectively as of Sept. 30, 2021. In FY 2021, there were six categories of material weaknesses (MWs) with the associated Notices of Findings and Recommendations (NFRs): Accounts Receivable/Revenue (3); Accounts Payable/Expense (11); Budgetary Resources (8); Fund Balance with Treasury (12); Financial Reporting (3); and Internal Controls (3). Based upon the results of the assessment, DISA is unable to provide assurance that internal controls over reporting are operating effectively as of Sept. 30, 2021.

DISA conducted its assessment of the effectiveness of internal controls over operations in accordance with OMB Circular No. A-123, the GAO Green Book, and the FMFIA. The *"Internal Control Evaluation (Appendix C)"* section provides specific information on how DISA conducted this assessment. This internal review also included an evaluation of the internal controls around our SAA activities. Based on the results of the assessment, DISA can provide reasonable assurance that internal controls over operations and compliance are operating effectively as of Sept. 30, 2021.

DISA conducted its assessment of the effectiveness of internal controls over reporting (including internal and external financial reporting) in accordance with OMB Circular No. A-123, Appendix A. The *"Internal Control Evaluation (Appendix C)"* section provides specific information on how DISA conducted this assessment. This assessment did not include an evaluation of the internal controls around our SAA activities because the financial reporting function is not yet in place for SAA for DISA as an implementing agency; however, related to SAA, DISA reported one self-reported MW (disbursement data used as receipt of services) in FY 2020, and that has not been remedied in FY 2021. In FY 2021, DISA reported one self-identified SD (Government Property in Possession of Contractors) and one self-identified MW (improper breakout of General Fund federal/non-federal undistributed balances). There were six categories of MWs with the associated NFRs: Accounts Receivable/Revenue (3); Accounts

Payable/Expense (11); Budgetary Resources (8); Fund Balance with Treasury (12); Financial Reporting (3); and Internal Controls (3). Based on the results of the assessment, DISA is unable to provide assurance that internal controls over reporting (including internal and external reporting as of Sept. 30, 2021), and compliance are operating effectively as of Sept. 30, 2021. Details are in the NFR database and available to interested parties.

DISA also conducted an internal review of the effectiveness of the internal controls over the integrated financial management systems in accordance with FMFIA and OMB Circular No. A-123, Appendix D. The *"Internal Control Evaluation" (Appendix C)* section provides specific information on how DISA conducted this assessment. This internal review included an evaluation of the internal controls around our SAA activities leveraging DISA's financial management systems structure. Based on the results of this assessment, DISA can provide reasonable assurance that the internal controls over the financial systems are in compliance with the FMFIA, Section 4; FFMIA, Section 803; and OMB Circular No. A-123, Appendix D, as of Sept. 30, 2021.

DISA has assessed entity-level controls, including fraud controls in accordance with the Green Book, OMB Circular No. A-123, the Payment Integrity Act of 2019, and GAO Fraud Risk Management Framework. This internal review included an evaluation of the internal controls for SAA activities encompassing DISA's overall fraud controls structure. Based on the results of the assessment, DISA can provide reasonable assurance that entity-level controls including fraud controls are operating effectively as of Sept. 30, 2021.

DISA is hereby reporting that no Antideficiency Act (ADA) violation has been discovered/identified during our assessments of the applicable processes.

If there are any questions regarding this statement of assurance for FY 2021, my point of contact is Mr. Richard (Greg) Swonger who can be reached at richard.g.swonger.civ@mail.mil or (614) 692-8596.

ROBERT J. SKINNER
Lieutenant General, USAF
Director

Attachments:
As stated

Financial Management Systems Framework, Goals, and Strategies

DISA's financial system implementations have been planned and designed within the framework of the Business Enterprise Architecture (BEA) established within the DoD, which facilitates to the extent possible a more standardized framework for systems in the department. Financial system-related initiatives target implementation of a standardized financial information structure that will be compliant with FFMIA and BEA requirements, and provide DISA with cost accounting data and timely accounting information that enable enhanced decision-making.

During FY 2021, DISA continued to operate and enhance the FAMIS, which supports the full breadth of DISA's WCF lines of business. In addition to the accounting system, DISA's financial systems environment is complemented by a select group of integrated financial tools and capabilities. These include:

- The functionality to provide customer and internal users with the ability to view details behind their telecommunication and contract IT invoices.
- A WCF information/execution management tool that provides users with the ability to view financial and non-financial (workload) data/consumption at a detailed level and provides a standardized method for cost allocations, budget preparation, rate development, and execution tracking with on-demand reports, ad-hoc queries, and table proof listings for analysis and decision-making.
- A web-based WCF budgeting system and financial dashboard that allows program financial managers to formulate budgets, project future estimates, prepare required budget exhibits, and monitor budget execution.
- A financial dashboard on a web-based business intelligence platform that enables users across the enterprise to access financial information for DWCF funds through static reports, interactive data cubes, and customizable dashboards.

These capabilities combined with key interfaces to acquisition, contracting, and ordering systems, underpin DISA’s automated framework of financial budgeting, execution, accounting, control, and reporting. Moving forward, DISA continues to solution improvements to its suite of financial tools by leveraging new technologies, evaluating opportunities to eliminate functional duplication where it exists, and reducing the footprint (and associated costs) of business systems writ large.

In that regard, DISA’s Strategic Plan contains an objective to “reform the agency.” Specifically, the plan addresses the agency’s financial systems strategy and dictates that DISA increase its use of technologies such as robotic process automation (RPA) and implement new technologies, such as artificial intelligence to “improve and automate financial and contractual transactions.” As a result of DISA’s experience using its newly modernized/compliant accounting systems for the previous two years, its accounting operations have stabilized. Accordingly, it is now taking advantage of its new capabilities to improve accounting processes and audit readiness, and to set the course for further financial modernization efforts across its business ecosystem. This includes identifying and assessing opportunities to sunset older legacy supporting systems by consolidating and/or migrating functionality to more modern and flexible technologies and architectures.

These advancements, as well as future accounting system improvements (e.g., implementing the One Fund concept, incorporating functionality to support Treasury’s G-Invoicing requirements, and supporting continued evolution of the BEA framework) will result in increased automation, transparency, access, and control of financial information in support of financial managers, mission partners, and higher echelon leaders.

5. Forward Looking

The DoD Joint Information Environment (JIE) is designed to create an enterprise information environment that optimizes use of the DoD IT assets, converging communications, computing, and enterprise services into a single joint platform that can be leveraged for all department missions. These efforts improve mission effectiveness, reduce total cost of ownership, reduce the attack surface of our networks, and enable DISA's mission partners to more efficiently access the information resources of the enterprise to perform their missions from any authorized IT device anywhere in the world. DISA continues its efforts towards realization of an integrated department-wide implementation of the JIE through development, integration, and synchronization of JIE technical plans, programs, and capabilities.

DISA is uniquely positioned to provide the kind of streamlined, rationalized enterprise solutions the department is looking for to effect IT transformation. DISA owns/operates enterprise and cloud-capable DISA Data Centers, the worldwide DISN, and the DITCO. DISA Data Centers routinely see workload increases — this trend will increase as major new initiatives begin to fully impact the department. As part of the department's transition to the JIE, DISA Data Centers have been identified as continental United States (CONUS) Core Data Centers (CDCs).

DISA also anticipates continuation of partnerships with other federal agencies. The DoD/Veterans Affairs Integrated Electronic Health Record (iEHR) agreement to host all medical records in DISA Data Centers and the requirement for DoD to provide Public Key Infrastructure (PKI) services to other federal agencies on a reimbursable basis are examples. We continue to move forward on several new initiatives, including:

- Accelerated implementation of MPLS technology.

- Deploying and sustaining Joint Regional Security Stacks (JRSS) to fundamentally change the way the DoD secures and protects its information networks.

- Operating a Joint Enterprise License Agreement (JELA) line of business with a low fee, a new management concept in Computing Services that aligns like functions across a single computing enterprise to prioritize excellence in service delivery, process efficiency, and standardization.

- The establishment of an on-premise cloud hosting capability to enable the department's migration to cloud computing.

- A reduced data footprint.

- Streamlined cybersecurity infrastructure; and the convergence of DoD networks, service desks, and operations centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives called Fourth Estate Network Optimization (4ENO).

- The establishment of an impact Level 5 cloud-based collaboration and productivity environment for Fourth Estate agencies and combatant commands.

- The enterprise-wide roll-out of a Cloud-Based Internet Isolation (CBII) capability that isolates malicious code and content from DoD networks.

DISA has implemented the Computing Ecosystem to support computing services for mission partners worldwide. This model aligned like functions across a single computing enterprise and established a unified computing structure operating under a single command — one large virtual data center. The Ecosystem prioritizes excellence in service delivery, process efficiency, and standardization for tools and processes. Ultimately, the shift to the Ecosystem model is fulfilling the goal of providing excellence in IT service delivery to our mission partners through the provision of cutting-edge computing solutions and a flexible and adaptable infrastructure. These optimization efforts are projected to yield a savings of $695 million over 10 years.

6. Limitations of the Financial Statements

The principal financial statements are prepared to report the financial position, financial condition, and results of operations, pursuant to the requirements of 31 U.S.C. § 3515(b). The statements are prepared from records of federal entities in accordance with federal Generally Accepted Accounting Principles (GAAP) and the formats prescribed by OMB. Reports used to monitor and control budgetary resources are prepared from the same records. Users of the statements are advised that the statements are for a component of the U.S. government.

The statements should be read with the realization that they are for a defense agency of the U.S. government, a sovereign entity.

Defense Information Systems Agency
Working Capital Fund
Principal Statements
Fourth Quarter of Fiscal Year 2021, Ending Sept. 30, 2021

Department of Defense
Defense Information Systems Agency WCF
As of Sept. 30, 2021 and 2020
($ in thousands)

Figure 19-Balance Sheet

	2021	2020 Consolidated
Intragovernmental:		
Fund Balance with Treasury (Note 3)	$ 213,653	$ 197,522
Accounts receivable, Net (Note 6)	894,403	964,161
Other Assets	-	841
Total Intragovernmental	1,108,056	1,162,524
Other than intragovernmental assets:		
Accounts receivable, net (Note 6)	990	1,596
General property, plant and equipment, net (Note 10)	908,288	890,604
Advances and prepayments (Note 12)	401	-
Total other than intragovernmental	909,679	892,200
Total Assets	$ 2,017,735	$ 2,054,724
Liabilities (Note 13)		
Intragovernmental:		
Accounts payable (Note 17)	$ 23,860	$ 26,266
Other Liabilities (Notes 15 and 17)	5,932	4,736
Total intragovernmental	29,792	31,002
Other than intragovernmental liabilities:		
Accounts payable	950,477	887,085
Federal employee and veteran benefits payable (Note 15)	6,012	4,363
Other Liabilities (Notes 17, 18 and 19)	57,541	52,486
Total other than intragovernmental	1,014,030	943,934
Total liabilities	1,043,822	974,936
Commitments and contingencies (Note 19)		
Net Position:		
Cumulative Results of Operations – Funds Other than Dedicated Collections	973,913	1,079,788
Total Cumulative Results of Operations	973,913	1,079,788
Total net position	973,913	1,079,788
Total liabilities and net position	$ 2,017,735	$ 2,054,724

*The accompanying notes are an integral part of these statements.

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2021 and 2020
($ in thousands)

Figure 20-Statement of Net Cost

Gross Program Costs (Note 21, Note 38)	**2021**	**2020 Consolidated**
Gross Costs (Note 24)	$ 8,383,736	$ 8,070,483
Less: Earned Revenue (Note 23)	(8,105,542)	(7,627,692)
Net Cost of Operations	278,194	442,791
Information Technology Contracts	4,172,229	4,069,080
Enterprise License Agreements	720,838	639,398
Reimbursable Telecommunications Services	890,296	840,746
Telecommunications Contracts	748,176	725,828
Other Programs	1,852,197	1,795,431
Less: Earned Revenue	(8,105,542)	(7,627,691)
Net Other Program Costs	$ 278,194	$ 442,791

*The accompanying notes are an integral part of these statements.

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2021 and 2020
($ in thousands)

Figure 21-Statement of Changes in Net Position

CUMULATIVE RESULTS OF OPERATIONS	2021	2020 Consolidated
Beginning Balance	$1,079,789	$1,247,458
Beginning Balances, as adjusted (includes Funds from Dedicated Collections)	1,079,789	1,247,458
Non-exchange revenue (Note 44)	-	(1)
Transfers-in/out without reimbursement	115,419	219,356
Imputed financing	56,900	55,767
Other	(1)	-
Net Cost of Operations (Includes Funds from Dedicated Collections)	278,194	442,791
Net Change in Cumulative Results of Operations (Includes Funds from Dedicated Collections)	(105,876)	(172,045)
Cumulative Results of Operation (Includes Funds from Dedicated Collections)	973,913	1,075,413
Net Position	$ 973,913	$1,075,413

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2021 and 2020
($ in thousands)

Figure 22-Statement of Budgetary Resources

	2021	2020 Consolidated
Budgetary Resources		
Unobligated balance from prior year budget authority, Net	$ 358,978	$ 823,763
Contract Authority (discretionary and mandatory) (Note 27)	135,319	232,951
Spending Authority from offsetting collections	6,463,955	6,194,516
Total Budgetary Resources	6,958,252	7,251,230
Status of Budgetary Resources		
New obligations and upward adjustments (total) (Note 28)	6,859,888	6,896,513
Apportioned, unexpired accounts	98,364	354,717
Unexpired unobligated balance, end of year	98,364	354,717
Unobligated balance, end of year (total)	98,364	354,717
Total Budgetary Resources	6,958,252	7,251,230
Outlays, Net		
Outlays, net (total) (discretionary and mandatory) (Note 38)	(16,131)	337,744
Agency Outlays, net (discretionary and mandatory)	$ (16,131)	$ 337,744

*The accompanying notes are an integral part of these statements.

Defense Information Systems Agency
Working Capital Fund
Notes to the Principal Statements
Fourth Quarter of Fiscal Year 2021, Ending Sept. 30, 2021

DEFENSE INFORMATION SYSTEMS AGENCY
WORKING CAPITAL FUND

Notes to the Principal Statements
Fourth Quarter of Fiscal Year 2021, Ending Sept. 30, 2021

Note 1. Summary of Significant Accounting Policies

Reporting Entity

DISA, a combat support agency within the Department of Defense (DoD), is a "Component Reporting Entity" (as defined by the Statement of Federal Financial Account Standards (SFFAS) 47), and consolidated into the DoD's financial statements.

The DoD includes the OSD, JCS, DoD Office of the Inspector General, military departments, defense agencies, DoD field activities, and combatant commands, which are considered and may be referred to as DoD components. The military departments consist of the Departments of the Army, Navy (of which the Marine Corps is a component), and the Air Force (of which the Space Force is a component). Appendix A provides a list of the components which comprises the Department's reporting entity for the purposes of these financial statements.

DISA provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to the joint warfighter, national-level leaders, and other mission and coalition partners across a full spectrum of operations. DISA implements the secretary of defense's defense strategic guidance and reflects the DoD CIO capability planning guidance.

Using the definitions and Appendix B Flowchart contained in SFFAS 47, DISA WCF has determined that there are not any other consolidation or disclosure entities or related transactions that are required to be disclosed within these notes.

Accounting Principles

The DISA WCF financial statements and supporting trial balances are compiled from the underlying financial data and trial balances within the WCF's sub-entities.

The DISA WCF presents the Balance Sheet, Statement of Net Cost, and Statement of Changes in Net Position that is a summation of the Components less the Eliminations. The Statement of Budgetary Resources is a summary of the DoD components and presented on a combined basis. Under the Statement of Budgetary Resources, intradepartmental activity has not been eliminated. However, the intra-DISA WCF balances for business between the TSEAS and CS business components has been eliminated to move the DISA WCF into a single fund (subhead/limit). The table below provides the impact of this change by USSGL.

Figure 23-Intra-DISA WCF One Fund Adjustment

(thousands)

	Normal D/C	Debit Amount	Credit Amount
1310-Accounts Receivable	Debit	$ -	$ 97,694
2110-Accounts Payable	Credit	97,694	-
4210-Anticipated Reimbursements	Debit	-	-
4221-Unfilled Customer Orders without Advance	Debit	-	1,085,912
4251-Reimbursements and Other Income Earned-Receivable	Debit	-	97,694
4590-Apportionments	Credit	-	-
4610-Allotsments-Realized Resources	Credit	34,829	-
4700-Commitments	Credit	772	-
4801-Undelivered Orders-Obligations, Unpaid	Debit	1,056,540	-
4871-Downward Adjustments of prior year Unpaid UDOs	Credit	-	6,230
4901-Delivered Orders-Obligations, Unpaid	Credit	97,694	-
5200-Revenue	Credit	936,610	-
6100-Expense	Debit	-	936,610

Figure 24-Intra-DISA WCF Collection and Outlay One Fund Adjustment

(thousands)

	Normal D/C	Debit Amount	Credit Amount
4210-Anticipated Reimbursements and Other Income	Debit	$ -	$ -
4902- Delivered Orders-Obligations, Paid	Credit	944,514	-
4252-Reimbursements and Other Income Earned-Collected	Debit	-	944,514
4590-Apportionment- Anticipated Resources	Credit	$ -	$ -

The DISA WCF adopted updated accounting standards and other authoritative guidance issued by the Federal Accounting Standards Advisory Board (FASAB) as listed below:

1) *SFFAS 50*: *Establishing Opening Balances for General Property, Plant, and Equipment Amending SFFAS 6, 10, and 23, and Rescinding SFFAS 35.* Issued on Aug. 4, 2016. Effective Date: For periods beginning after Sept. 30, 2016. (See Note 10)

2) *SFFAS 53: Budget and Accrual Reconciliation, Amending SFFAS 7 and 24, and Rescinding SFFAS 22*. Issued on Oct. 27, 2017; Effective for periods beginning after Sept. 30, 2018.

3) *Technical Bulletin 2020-1*: *Loss Allowance for Intragovernmental Receivables*. Issued Feb. 20, 2020.

DISA WCF implemented Standard Financial Information Structure (SFIS) compliant accounting systems and improved processes based on independent reviews and compliance with OMB Circular No. A-136 and U.S. Generally Accepted Accounting Principles.

Financial statements outline key funding for a component of the U.S. government. Some assets and liabilities can be offset by a different entity, thereby eliminating it from government-wide reporting.

Fund Balance with Treasury

The FBWT represents the aggregate amount of the DISA WCF's available budget spending authority, which is accessible to pay current liabilities and finance future purchases. DISA's monetary resources of collections and disbursements are maintained in Department of the Treasury (Treasury) accounts. The disbursing offices of the DFAS, the military departments, the U.S. Army Corps of Engineers (USACE), and the Department of State's financial service centers process majority of the DoD's cash collections, disbursements, and adjustments worldwide. Each disbursing station reports to the Treasury on checks issued, electronic fund transfers, interagency transfers, and deposits.

FBWT is an asset of a component entity and a liability of the Treasury General Fund. Similarly, investments in government securities held by dedicated collections accounts are assets of the reporting entity responsible for the dedicated collections and liabilities of the Treasury GF. In both cases, the amounts represent commitments by the government to provide resources for particular programs, but they do not represent net assets to the government as whole.

When a reporting entity seeks to use FBWT or investments in government securities to liquidate budgetary obligations, Treasury will finance the disbursements by borrowing in the same way it finances all other disbursements from the public if there is a budget deficit (or use current receipts if there is a budget surplus).

Additionally, the DoD reports to the Treasury Department by appropriation on interagency transfers, collections received, and disbursements issued. The Treasury records these transactions to the applicable Fund Balance with Treasury.

Treasury and trial balance amounts include inception to date balances and are used for Treasury baselines and reconciliations. Methodology incorporates comparison of Treasury and trial balance transactions to reconcile, identify, and explain the differences between account balances. The DoD policy is to allocate and apply supported differences (undistributed disbursements and collections) to reduce accounts payable and receivable accordingly. Differences, or reconciling items, may be caused by the timing of transactions, an invalid line of accounting, or insufficient detail.

The DISA Working Capital Fund FBWT balance is reconciled monthly to the amounts reported in the CMR, which represents DISA's portion of the FBWT balance reported by the Treasury Department. The settlement process incorporates a baseline reconciliation performed during fiscal year 2005. The baseline reconciliation included activity from the revolving fund's inception in fiscal year 1994, to which DISA reconciled balances from legacy accounting systems previously purged during accounting system migration. Therefore, alternative settlement methods were performed to reconcile amounts reported by Treasury in those fiscal years to official accounting reports. Since FY 2005, DISA has reconciled FBWT amounts reported by Treasury, as identified in the CMR, at the transaction level and on a monthly basis. No further settlement items that predate the baseline reconciliation have surfaced.

DISA WCF does not report deposit fund balances on its financial statements.

For additional information, see Note 3 *Fund Balance with Treasury.*

Revenue and Other Financing Sources

The financial transactions resulting from the budget process are generally the same transactions reflected in agency and the government-wide financial reports.

The department's budgetary resources reflect past congressional action and enable the entity to incur budgetary obligations, but do not reflect assets to the government as a whole. Budgetary obligations are legal obligations for goods, services, or amounts to be paid based on statutory provisions (e.g., Social Security benefits). After budgetary obligations have incurred, Treasury will make disbursements to liquidate the budgetary obligations and finance those disbursements.

The DoD receives congressional appropriations and funding as general, working capital (revolving), trust and special funds. The Department uses these appropriations and funds to execute its missions and subsequently report on resource usage.

WCFs conduct business-like activities and receive funding to establish an initial corpus through an appropriation or a transfer of resources from existing appropriations or funds. The corpus finances operations and transactions flowing through the fund. Each WCF obtains the goods and services sold to customers on a reimbursable basis and maintains the corpus. Reimbursable receipts fund future operations and generally are available in their entirety for use without further congressional action. At various times, Congress provides additional appropriations to supplement the WCF as an infusion of cash when revenues are inadequate to cover costs within the corpus.

In accordance with SFFAS Number 7 "Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting," the DISA WCF recognizes exchange revenue using the service-type revenue recognition policy. Under this method, revenue is considered earned and recognized, along with associated costs, at the time the service is rendered or performed, and not less frequently than monthly. These exchange revenues reduce the cost of operations. The DISA WCF's pricing policy for reimbursable agreements is to recover full cost and should result in no profit or loss (breakeven) within planned timeframes based on budget and planning projections.

Deferred revenue is recorded when the DoD receives payment for goods or services which have not been fully rendered. Deferred revenue is reported as a liability on the Balance Sheet until earned.

The DoD does not include non-monetary support provided by U.S. allies for common defense and mutual security in amounts reported in the Statement of Net Cost. The U.S. has cost sharing agreements with countries, through mutual or reciprocal defense agreements, where U.S. troops are stationed or a U.S. fleet is ported.

Changes in Entity or Financial Reporting

Previously, a subset of diverse assets that did not lend themselves to a single activation date, depreciation was calculated using a composite method mid-year type approach. This was done by commencing depreciation expense for the assets because at the time it provided the most systematic and rational approach to applying an asset activation date. The date chosen was not the actual mid-year point of the fiscal year, but rather June 30 of each year because the third and fourth quarters of the FY consistently represent the periods of highest activity for receipt of equipment. The DISA WCF has now developed a

capability to determine a more precise asset activation date using a month available for service method for assets. Associated depreciation expenses can now be calculated to match a period in which a benefit is derived, as required to meet accounting standards.

Classified Activities

Accounting standards allow certain presentations and disclosures to be modified, if needed, to prevent the disclosure of classified information.

Fiduciary Activities

DISA WCF does not have fiduciary activities.

Parent-Child Reporting

DISA WCF is not party to allocation transfers with other federal agencies.

Pension, ORB, and OPEB Reporting

DISA WCF does not administer pensions, other reportable benefits (ORB), or other post-employment benefits (OPEB), and does not report gains or losses on retirement benefits.

The DoD applies SFFAS 33, Pensions, Other Retirement Benefits, and Other Postemployment Benefits: Reporting the Gains and Losses from Changes in Assumptions and Selecting Discount Rates and Valuation Dates, when selecting the discount rate and valuation date used to estimate military retirement benefit actuarial liabilities. In addition, gains and losses from changes in long-term assumptions used to estimate the actuarial liability are presented separately on the DoD Statement of Net Cost. Refer to Note 15, *Federal Employee and Veteran Benefits Payable* and Note 20, *Disclosures Related to the Statement of Net Cost*, for additional information.

As an employer entity, the DISA WCF recognizes the annual cost of its civilian employees' pension, other retirement benefit plans, and other postemployment benefit plans (plans) including health and life insurance plans. However, as the administering entity, OPM is responsible for executing the benefit plans including accounting for plan assets, liabilities and associated gains and losses. Accordingly, the DISA WCF does not display gains and losses from changes in long-term assumptions used to measure these liabilities on the Statement of Net Cost.

The majority of DoD employees hired prior to Jan. 1, 1984, participate in the Civil Service Retirement System (CSRS), while most DoD employees hired after Dec. 31, 1983, are covered by the Federal Employees Retirement System (FERS) and Social Security. Employees hired between Jan. 1, 1984 and Dec. 31, 2012 are covered by the FERS basic annuity benefit. FERS also offers a defined contribution plan (Thrift Savings Plan) as a primary feature, to which the department automatically contributes 1 percent of base pay and matches employee contributions up to an additional 4 percent of base pay. The department also contributes to the employer's Social Security matching share for FERS participants.

Similar to CSRS and FERS, OPM reports the liability for future payments to retired employees who participate in the Federal Employees Health Benefits Program and Federal Employees Group Life Insurance Program. The department reports both the full annual cost of providing these ORB for its retired employees and reporting contributions made for active employees. In addition, the department recognizes the cost for OPEB, including all types of benefits provided to former or inactive (but not

retired) employees, their beneficiaries and covered dependents.

The difference between the full annual cost of CSRS and FERS retirement, ORB, and OPEB and the amount paid by the department is recorded as an imputed cost and offsetting imputed financing source in the accompanying financial statements.

Statement of Social Insurance (SOSI) Reporting

DISA WCF does not participate in social insurance programs and thus does not prepare a Statement of Social Insurance (SOSI).

Note 2. Non-entity Assets

Non-entity assets are assets for which the DISA WCF maintains stewardship accountability and reporting responsibility but are not available for WCF normal operations.

DISA WCF non-entity assets are composed of immaterial amounts (rounded to zero $000) of accumulated interest receivable, and accumulated penalties and administrative fees receivable as reported in the Monthly Debt Management Report Contract Debt System. The DFAS initiates collection actions and transfers collected funds to the Treasury after receipt of payment.

Total entity assets for the DISA WCF are comprised of FBWT, accounts receivable, general property, plant and equipment, and advances and prepayments-other assets.

Figure 25-Non-Entity Assets

(thousands)

	2021	2020
1. **Intragovernmental Assets**		
A. Fund Balance with Treasury	$ -	$ -
B. Accounts Receivable	-	-
C. Other Assets	-	-
D. Total Intragovernmental Assets	$ -	$ -
2. **Non-Federal Assets**		
A. Cash and Other Monetary Assets	$ -	$ -
B. Accounts Receivable	-	-
C. Other Assets	-	-
D. Total Non-Federal Assets	$ -	$ -
3. **Total Non-Entity Assets**	$ -	$ -
4. **Total Entity Assets**	$ 2,017,735	$ 2,054,724
5. **Total Assets**	$ 2,017,735	$ 2,054,724

Note 3. Fund Balance with Treasury

COVID-19 Impacts

Please see Note 42

Status of Fund Balance with Treasury

DISA WCF's Fund Balance with Treasury consists of revolving funds provided from the initial cash corpus, supplemental appropriations, and revolving funds from operations.

The Status of FBWT reflects the reconciliation between the budgetary resources supporting FBWT (largely consisting of unobligated balance and obligated balance not yet disbursed) and those resources provided by other means. The total FBWT reported on the Balance Sheet reflects the budgetary authority remaining for disbursements against current or future obligations.

The unobligated balance available amount of $98.4 million represents the cumulative amount of budgetary authority set aside to cover future obligations and is not restricted for future use. The available balance consists primarily of the unexpired, unobligated balance that has been apportioned and available for new obligations.

Obligated balance not yet disbursed in the amount of $1.8 billion represents funds obligated for goods and services but not paid.

Non-budgetary FBWT includes accounts without budgetary authority, such as deposit funds, unavailable receipt accounts, clearing accounts and non-entity FBWT. The DISA WCF does not have any balances to report as non-budgetary FBWT.

The Non-FBWT budgetary accounts in the amount of $1.7 billion reduces budgetary resources and is primarily composed of unfilled customer orders without advance from customers in the amount of $723.7 million, Contract Authority in the amount of $192.8 million, and Receivables and Other in the amount of $802.6 million.

Contract authority and reimbursable authority (spending authority from anticipated collections) does not increase the FBWT when initially posted, but does provide budgetary resources. FBWT increases only after the customer payments for services or goods rendered have been collected.

Unfilled customer orders without advance and reimbursements and other income earned - receivable provide budgetary resources when recorded. FBWT is only increased when reimbursements are collected, not when orders are accepted or earned.

The FBWT reported in the financial statements has been adjusted to reflect DISA WCF's balance as reported by Treasury and identified to DISA WCF on the CMR. The difference between FBWT in the DISA WCF general ledgers and FBWT reflected in the Treasury accounts is attributable to transactions that have not been posted to the individual detailed accounts in WCF's general ledger as a result of timing differences or the inability to obtain valid accounting information prior to the issuance of the financial statements. When research is completed, these transactions will be recorded in the appropriate individual detailed accounts in DISA WCF's general ledger accounts.

Figure 26-Fund Balance with Treasury

(thousands)

DISA WCF	2021	2020
1. Unobligated Balance:		
A. Available	$ 98,364	$ 354,717
B. Unavailable	-	-
Total Unobligated Balance	98,364	354,717
2. Obligated Balance not yet Disbursed	1,834,349	3,144,977
3. Non-Budgetary FBWT:		
A. Clearing accounts	-	-
B. Deposit funds	-	-
C. Non-entity and other	-	-
Total Non-Budgetary FBWT	-	-
4. Non-FBWT Budgetary Accounts:		
A. Investments – Treasury Securities	-	-
B. Unfilled Customer Orders without Advance	(723,650)	(2,098,480)
C. Contract Authority	(192,841)	(219,286)
D. Borrowing Authority	-	-
E. Receivables and Other	(802,569)	(984,407)
Total Non-FBWT Budgetary Accounts	(1,719,060)	(3,302,173)
5. Total FBWT	$ 213,653	$ 197,521

Note 6. Accounts Receivable, Net

COVID-19 Impacts

Please see Note 42

Accounts receivable represent the DISA WCF's claim for payment from other entities. Claims with other federal agencies are resolved in accordance with the business rules published in Appendix 5 of Treasury Financial Manual, Volume I, Part 2, Chapter 4700. Allowances for uncollectable accounts receivable are based on an analysis of aged accounts receivable.

Figure 27-Accounts Receivable, Net

(thousands)

DISA WCF 2021	Gross Amount Due	Allowance for Estimated Uncollectibles	Accounts Receivable, Net
Intragovernmental Receivables	$ 901,028	$ (6,624)	$ 894,404
Non-Federal Receivables (From the Public)	990	(1)	989
Total Accounts Receivable	$ 902,018	$ (6,625)	$ 895,393

DISA WCF 2020	Gross Amount Due	Allowance for Estimated Uncollectibles	Accounts Receivable, Net
Intragovernmental Receivables	$ 964,161	$ -	$ 964,161
Non-Federal Receivables (From the Public)	1,596	-	1,596
Total Accounts Receivable	$ 965,757	$ -	$ 965,757

Note 10. General Property, Plant and Equipment, Net

COVID-19 Impacts

Please see Note 42

DISA WCF General PP&E comprises telecommunications and computing services with related equipment, software, leasehold improvements, construction-in-progress and assets under capital lease with a net book value (NBV) of $908.3 million.

DISA WCF uses historical cost for determining General PP&E beginning balances, not deemed cost as provided by SFFAS 50 – *Establishing Opening Balances for General Property, Plant, and Equipment.*

There are no restrictions on the use or convertibility of the DISA WCF's property and equipment and all values are based on acquisition cost.

The DISA WCF does not possess any Stewardship PP&E (Federal Mission PP&E, Heritage Assets, or Stewardship Land).

The following tables provide a summary of the activity for the current and prior FY.

Figure 28-General Property, Plant, and Equipment, Net

(thousands)

	CY	PY
General PP&E, Net beginning of year	$ 890,603	$ 804,827
Capitalized Acquisitions	142,786	92,542
Dispositions	(13,789)	-
Transfers in/(out) without reimbursement	115,397	-
Revaluations (+/-)	-	227,193
Depreciation Expense	(226,710)	(233,960)
Donations	-	-
Other (+/-)	-	-
Balance at end of year	$908,287	$890,602

The charts below provide the depreciation method, service life, acquisition value, depreciation, and net book value for the different categories in a comparative view.

Figure 29-Major General PP&E Asset Classes

(thousands)

DISA WCF 2021 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
A. Land	N/A	N/A	$ -	$ -	$ -
B. Buildings, Structures, and Facilities	S/L	35, 40, or 45*	-	-	-
C. Leasehold Improvements	S/L	Lease term	20,932	(10,290)	10,642
D. Software	S/L	2-5 or 10	197,204	(124,743)	72,461
E. General Equipment	S/L	Various*	2,310,252	(1,570,391)	739,861
F. Assets Under Capital Lease	S/L	Lease term	363,716	(300,122)	63,594
G. Construction-in-Progress	N/A	N/A	21,730	N/A	21,730
H. Other	N/A	N/A	-	-	-
I. Total General PP&E			$ 2,913,834	$ (2,005,546)	$ 908,288

DISA WCF 2020 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
A. Land	N/A	N/A	$ -	$ -	$ -
B. Buildings, Structures, and Facilities	S/L	35, 40, or 45*	-	-	-
C. Leasehold Improvements	S/L	Lease term	13,771	(10,494)	3,277
D. Software	S/L	2-5 or 10	192,717	(95,554)	97,163
E. General Equipment	S/L	Various*	2,123,277	(1,443,321)	679,956
F. Assets Under Capital Lease	S/L	Lease term	363,716	(291,580)	72,136
G. Construction-in-Progress	N/A	N/A	38,071	N/A	38,071
H. Other	N/A	N/A	-	-	-
I. Total General PP&E			$ 2,731,552	$ (1,840,949)	$ 890,603

Legend for Valuation Methods:
S/L=Straight Line N/A= Not Applicable
*Estimated useful service life is 35 years for structures, 40 years for linear structures, and 45 years for buildings.

Note 12. Other Assets

COVID-19 Impacts
Please see Note 42

Intragovernmental advances and prepayments decreased $841 thousand because of an adjustment to reconcile trading partner data. In the current fiscal year, total other assets are shown as zero due to mapping changes presented on the balance sheet.

Figure 30-Other Assets

(thousands)

	2021	2020
1. Intragovernmental Other Assets		
A. Advances and Prepayments	$ -	$ 841
B. Other Assets	-	-
C. Total Intragovernmental Other Assets	-	841
2. Other than Intragovernmental		
A. Outstanding Contract Financing Payments	-	-
B. Advances and Prepayments	401	-
C. Other Assets (With the Public)	-	-
D. Subtotal	401	-
E. Less: "Outstanding Contract Financing Payments" and "Advance and Prepayments" totaled and presented on the balance sheet as "Advances and Prepayments"	(401)	-
5. Total Other Assets	$ -	$ 841

Note 13. Liabilities Not Covered by Budgetary Resources

COVID-19 Impacts
Please see Note 42

Liabilities not covered by budgetary resources include liabilities needing congressional action before budgetary resources are provided.

Intragovernmental liabilities-other comprises the DISA WCF's unfunded FECA liability in the amount of $1 million. These liabilities will be funded in future periods.

Other than intragovernmental liabilities-Federal employee and veteran benefits payable consist of various employee actuarial liabilities not due and payable during the current fiscal year. As of Sept. 30, 2021, the DISA WCF's liabilities consist of actuarial FECA liability for workers compensation benefits in the amount of $4.7 million. These liabilities will be funded in future periods.

Figure 31-Liabilities Not Covered by Budgetary Resources

(thousands)

DISA WCF	2021	2020
1. Intragovernmental Liabilities		
A. Accounts Payable	$ -	$ -
B. Debt	-	-
C. Other	1,009	1,070
Total Intragovernmental Liabilities	1,009	1,070
2. Other than Intragovernmental Liabilities		
A. Accounts Payable	-	-
B. Federal Employee and Veteran Benefits Payable	4,664	4,363
C. Environmental and Disposal Liabilities	-	-
D. Benefits due and payable	-	-
E. Other Liabilities	-	-
F. Total Other than Intragovernmental Liabilities	4,664	4,363
3. Total Liabilities Not Covered by Budgetary Resources	5,673	5,433
4. Total Liabilities Covered by Budgetary Resources	1,038,149	969,501
5. Total Liabilities Not Requiring Budgetary Resources	-	-
6. Total Liabilities	$ 1,043,822	$ 974,936

Note 15. Federal Employee and Veteran Benefits Payable

COVID-19 Impacts

Please see Note 42

Actuarial Cost Method Used and Assumptions:

The Department of Labor (DOL) estimates actuarial liability at the end of each fiscal year.

In FY 2020, the methodology for billable projected liabilities was revised to include, among other things: (1) an algorithmic model that relies on individual case characteristics and benefit payments (the FECA Case Reserve Model); (2) incurred but not reported claims were estimated using the patterns of incurred benefit liabilities in addition to those of payments. The FY 2019 methodology used a traditional paid-loss development method with the FECA Case Reserve Model running concurrently to test the validity of the FECA Case Reserve Model.

The effects of inflation on the liability for future workers' compensation benefits, wage inflation factors, cost of living adjustments (COLAs) and medical inflation factors consumer price index medical (CPI-Ms) were also applied to the calculation of projected future benefits.

DOL selected the COLA factors, CPI-M factors, and discount rate by averaging the COLA rates, CPI-M rates, and interest rates for the current and prior four years, all while using averaging render estimates that reflect historical trends over five years instead of opting for conditions that exist over one year.

The FY 2021 and FY 2020 methodologies for averaging the COLA rates used OMB-provided rates. The FY 2020 methodology also considered updated information provided by program staff. The FY 2021 and

FY 2020 methodologies for averaging the CPI-M rates used OMB-provided rates and information obtained from the Bureau of Labor Statistics public releases for CPI.

The actual rates for these factors for the charge back year (CBY) 2021 were also used to adjust the methodology's historical payments to current-year constant dollars. The compensation COLAs and CPI-Ms used in the projections for various CBY were as follows:

Figure 32- Compensation COLAs and CPI-Ms

CBY	COLA	CPI-M
2021	N/A	N/A
2022	2.11%	2.74%
2023	2.48%	3.15%
2024	2.55%	3.56%
2025	2.62%	3.49%
2026 and thereafter	2.68%	3.79%

DOL selected the interest rate assumptions, whereby projected annual payments were discounted to present value based on interest rate assumptions on the U.S. Department of the Treasury's Yield Curve for Treasury Nominal Coupon Issues (the TNC Yield Curve) to reflect the average duration of income payments and medical payments. Discount rates were based on averaging the TNC Yield Curves for the current and prior four years for FY 2021 and FY 2020, respectively. Interest rate assumptions utilized for FY 2021 discounting were as follows:

Discount Rates

For wage benefits:
2.231 percent in Year 1 and years thereafter;
For medical benefits:
2.060 percent in Year 1 and years thereafter.

To test the reliability of the model, comparisons were made between projected payments in the last year to actual amounts, by agency. Changes in the liability from last year's analysis to this year were also examined by agency, with any significant differences by agency inspected in greater detail. The model has been stable and has projected the actual payments by agency reasonably well.

The American Rescue Plan Act, P.L. 117-2, section 4016, "Eligibility for Workers' Compensation Benefits for Federal Employees Diagnosed with COVID-19," mandated that the FECA Special Benefits Fund assume an unreimbursed liability (i.e., a liability that is not chargeable to the agencies) for approved claims of certain covered employees for injuries proximately caused by exposure to the novel coronavirus that causes COVID-19 (or another coronavirus declared to be a pandemic by public health authorities) while performing official duties during the covered exposure period. Pursuant to section 4016, these claims must be accepted on or after March 12, 2021 and through Sept. 30, 2030 and cover benefits for disability compensation and medical services and survivor benefits. Accordingly, section 4016 future benefits are properly omitted from the table of Estimates of Total FECA Future Liabilities as of Sept. 30, 2021.

Expense Components

For FY 2021, the only expense component pertaining to other actuarial benefits for the DISA WCF is the FECA expense. The DOL provides the expense data to DISA. The staffing ratio data from DISA headquarters determines the allocation of the expense to DISA WCF.

The DOL provided an estimate for DISA's future workers' compensation benefits of $9.2 million in total, of which $4.7 million was distributed to the DISA WCF based upon staffing ratios. DISA made the distribution using DISA's normal methodology of apportioning FECA liability to WCF based upon relative staffing levels. DISA used the same apportionment methodology in prior years.

Changes in Actuarial Liability

Fluctuations in the total liability amount charged to DISA by DOL will cause changes in FECA liability. The Other Actuarial Benefits, FECA liability increased $300.4 thousand due to an increase in COLA and CPIM inflation factors that in turn increased the actuarial liability estimate provided by DOL (http://www.dol.gov/ocfo/publications.html).

Figure 33-Federal Employee and Veteran Benefits Payable

(thousands)

DISA WCF 2021	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
1. Pension and Health Benefits			
A. Military Retirement Pensions	$ -	$ -	$ -
B. Military Pre Medicare-Eligible Retiree Health Benefits	-	-	-
C. Military Medicare-Eligible Retiree Health Benefits	-	-	-
D. Total Pension and Health Benefits	-	-	-
2. Other Benefits			
A. FECA	4,664	-	4,664
B. Voluntary Separation Incentive Programs	-	-	-
C. DoD Education Benefits Fund	-	-	-
D. Other	1,347	(1,347)	-
E. Total Other Benefits	6,011	(1,347)	4,664
3. Federal Employee and Veteran Benefits Payable (presented separately on the Balance Sheet)	6,011	(1,347)	4,664
4. Other benefit-related payables included in Intragovernmental Accounts Payable on the Balance Sheet	-	-	-
5. Other benefit-related payables included in Intragovernmental Other Liabilities on the Balance Sheet	5,531	(4,522)	1,009
Total Federal Employee Benefits Payable	$ 11,542	$ (5,869)	$ 5,673

DISA WCF 2020	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
1. Pension and Health Benefits			
A. Military Retirement Pensions	$ -	$ -	$ -
B. Military Pre Medicare-Eligible Retiree Health Benefits	-	-	-
C. Military Medicare-Eligible Retiree Health Benefits	-	-	-
D. Total Pension and Health Benefits	-	-	-
2. Other Benefits			
A. FECA	4,363	-	4,363
B. Voluntary Separation Incentive Programs	-	-	-
C. DoD Education Benefits Fund	-	-	-
D. Other	-	-	-
E. Total Other Benefits	4,363	-	4,363
3. Federal Employee and Veteran Benefits Payable (presented separately on the Balance Sheet)	4,363	-	4,363
4. Other benefit-related payables included in Intragovernmental Accounts Payable on the Balance Sheet	-	-	-
5. Other benefit-related payables included in Intragovernmental Other Liabilities on the Balance Sheet	-	-	-
Total Federal Employee and Veteran Benefits Payable	$ 4,363	$ -	$ 4,363

Note 17. Other Liabilities

COVID-19 Impacts

Please see Note 42

Intragovernmental

Advances from others represent liabilities for collections received, that could impact future expenses or the acquisition of assets the DISA WCF incurs or acquires on behalf of another organization.

Other Than Intragovernmental

Accrued funded payroll and benefits – $57.5 million: The DISA WCF reports the unpaid portion of accrued funded civilian payroll and employee's annual leave as it is earned as other liabilities, and subsequently reduces the leave liability when it is used. Unused leave is an unfunded liability which will be paid from future resources when taken or when the employee retires or separates. The liability reported at the end of the accounting period reflects the current pay rates. When sick leave is earned, a liability is not recognized for unused amounts because employees do not vest in this benefit. Sick and holiday leave is expensed when taken.

Advances from others - $7 thousand: This liability primarily consists of decentralized contract orders whereby DISA customers place orders directly with vendors for which the DITCO fee is collected prior to being billed.

DISA life and other insurance programs covering civilian employees are provided through the OPM. DISA does not negotiate the insurance contracts and incurs no liabilities directly to insurance companies. Employee payroll withholdings related to the insurance and employer matches are submitted to OPM.

Figure 34-Other Liabilities

(thousands)

DISA WCF 2021	Current Liability	Non-Current Liability	Total
1. Intragovernmental	$ 401	$ -	$ 401
A. Advances from Others and Deferred Revenue	-	-	-
E. FECA Reimbursement to the Department of Labor			
F. Liabilities for Non-entity Assets	-	-	-
G. Employer Contribution and Payroll Taxes Payable	-	-	-
I. Subtotal	401	-	401
J. Other Liabilities reported on Note 13, *Federal Employee and Veterans Benefits Payable*	5,531	-	5,531
K. Total Intragovernmental	5,932	-	5,932
2. Other than Intragovernmental			
A. Accrued Funded Payroll and Benefits	57,534	-	57,534
B. Advances from Others	7	-	7
J. Employer Contribution and Payroll Taxes Payable	-	-	-
K. Contingent Liabilities	-	-	-
L. Other Liabilities without Related Budgetary Obligations	-	-	-
M. Other Liabilities without Related Budgetary Obligations	-	-	-
N. Total Other than Intragovernmental	57,541	-	57,541
3. Total Other Liabilities	$ 63,473	$ -	$ 63,473

DISA WCF 2020	Current Liability	Non-Current Liability	Total
1. Intragovernmental	$ -	$ -	$ -
A. Advances from Others and Deferred Revenue	550	521	1,071
E. FECA Reimbursement to the Department of Labor			
F. Liabilities for Non-entity Assets	-	-	-
G. Employer Contribution and Payroll Taxes Payable	3,665	-	3,665
I. Subtotal	4,215	521	4,736
J. Other Liabilities reported on Note 13, *Federal Employee and Veteran Benefits Payable*	-	-	-
K. Total Intragovernmental	4,215	521	4,736
2. Other than Intragovernmental			
A. Accrued Funded Payroll and Benefits	50,834	-	50,834
B. Advances from Others	939	-	939
J. Employer Contribution and Payroll Taxes Payable	714	-	714
K. Contingent Liabilities	-	-	-
L. Other Liabilities without Related Budgetary Obligations	-	-	-
M. Other Liabilities with related Budgetary Obligations	-	-	-
N. Total Other than Intragovernmental	52,487	-	52,487
3. Total Other Liabilities	$ 56,702	$ 521	$ 57,223

Note 18. Leases

Figure 35- Entity as Lessee - Assets Under Capital Lease (Table 16A)

(thousands)

	2021	2020
Land and Buildings	$ -	$ -
Equipment	363,716	363,716
Accumulated Amortization	(300,122)	(291,580)
Total Capital Lease	$ 63,594	$ 72,136

The DISA WCF records assets that meet the capital lease criteria defined by FASAB Statements of Federal Financial Accounting Standard No. 6. These assets represent agreements for the exclusive use of certain transoceanic cables in support of network communications as part of the optical transport network.

In prior fiscal years, the DISA WCF transferred in Defense Information Systems Network Core Program capital leases and accumulated amortization from the DISA GF. However, these leases were paid in full at inception removing the need for future lease payments and associated lease liability.

The DISA WCF does not currently have any future payments due for assets under capital lease.

The DISA WCF has operating leases for land, buildings and equipment. Future lease payments due as of Sept. 30, 2021, for non-cancelable operating leases were as follows:

Figure 36-Future Payments Due for Non-Cancelable Operating Leases (Table 16D)

(thousands)

DISA WCF 2021	Land & Buildings	Equipment	Other	Total
1. Federal				
Fiscal Year 2022	$ 896	$ 181	$ -	$ 1,077
Fiscal Year 2023	708	-	-	708
Fiscal Year 2024	732	-	-	732
Fiscal Year 2025	756	-	-	756
Fiscal Year 2026	780	-	-	780
After 5 years	1,070	-	-	1,070
Total Federal Future Lease Payments	4,942	181	-	5,123
2. Total Non-Federal Future Lease Payments	-	-	-	-
3. Total Future Lease Payments	$ 4,942	$ 181	-	$ 5,123

DISA WCF 2020	Land & Buildings	Equipment	Other	Total
1. Federal				
Fiscal Year 2021	$ 3,954	$ 531	$ -	$ 4,485
Fiscal Year 2022	3,280	-	-	3,280
Fiscal Year 2023	1,271	-	-	1,271
Fiscal Year 2024	1,313	-	-	1,313
Fiscal Year 2025	1,356	-	-	1,356
After 5 years	3,317	-	-	3,317
Total Federal Future Lease Payments	14,491	531	-	15,022
2. Total Non-Federal Future Lease Payments	-	-		-
3. Total Future Lease Payments	$ 14,491	$ 531	$ -	$ 15,022

Land and Building Leases

As of Sept. 30, 2021, the DISA WCF operates in 19 locations, of which 16 sites are located on property (primarily military bases) where no rent is charged and only utilities are required. The three remaining sites are located on both commercial and government-owned properties and covered under long-term real estate leases expiring at various dates through 2028. The DISA WCF acquires space for government-owned property through the General Services Administration, which acquires and manages most commercial property leases on behalf of the federal government. These leases generally require the DISA WCF to pay property taxes, utilities, security, custodial services, parking, and operating expenses. Certain leases contain renewal options.

Equipment Leases

Equipment leases are operating leases for photocopiers and vehicles. The DISA WCF currently leases 135 photocopiers and 23 vehicles located across various sites. The photocopiers are leased for three years, while the vehicles are leased for one year with annual renewal options.

Note 19. Commitments and Contingencies

COVID-19 Impacts
Please see Note 42

The DISA WCF is a party in various administrative proceedings and legal actions related to claims for environmental damage, equal opportunity matters, and contractual bid protests. The DISA WCF reviews the agency claims report and determines if a liability should be recorded for the reporting period. DISA WCF did not record any contingent liabilities for the fourth quarter of FY 2021 reporting.

Disclosures Related to the Statement of Net Cost

Note 21. Suborganization Program Costs

COVID-19 Impacts
Please see Note 42

The Statement of Net Cost (SNC) represents the net cost of programs and organizations the DISA WCF supported by other means. The intent of the SNC is to provide gross and net cost information related to the amount of output or outcome for a given program or organization (TSEAS and CS) administered by a responsible reporting entity. The CS and TSEAS program are elements of the WCF.

Intragovernmental costs and revenue are related to transactions between two reporting entities within the federal government. Public costs and revenue are exchange transactions made between the DISA WCF and a nonfederal entity.

The DISA WCF reports exchange revenues for earned inflows of resources. They arise from exchange transactions, which occur when each party involved in a transaction sacrifices value and receives value in return. Pricing policy for exchange revenue is derived from stabilized rates established to recover estimated operating expenses incurred for the applicable FY, and to provide sufficient working capital for the acquisition of fixed assets as approved by the under secretary of defense (comptroller). Stabilized rates and unit prices are established at levels intended to equate estimated revenues to estimated costs. When gains or losses occur in prior fiscal years from under or over applied stabilized rates and/or prices, those gains or losses are incorporated into a current year's stabilized rates. However, the estimated revenues may not equal estimated costs.

The following schedules supports the summary information presented in the SNC and discloses separate intragovernmental activity (transactions with other federal agencies) from transactions with the public. Costs incurred through the procurement of goods and services from both public and other federal agency providers, along with revenues earned from public and other federal customers, is shown for each line of business. As disclosed in Note 1.D, the costs incurred and revenue earned for DISA WCF programs that received and provided services to one another have been adjusted and is not reflected in the totals. The DISA WCF's services are priced to recover the full cost of resources consumed to produce the service.

Figure 37-General Disclosures Related to the Statement of Net Cost

(thousands)

DISA WCF	2021	2020
Operations, Readiness & Support		
Gross Cost	$ 8,383,736	$ 8,070,483
Less: Earned Revenue	(8,105,542)	(7,627,691)
Net Program Costs	278,194	442,791
Consolidated		
Gross Cost	8,383,736	8,070,483
Less Earned Revenue	(8,105,542)	(7,627,691)
Total Net Cost	$ 278,194	$ 442,791

The DoD implemented SFFAS 55 in FY 2018 which rescinds SFFAS 30 "Inter-entity Cost Implementation: Amending SFFAS 4, Managerial Cost Accounting Standards and Concepts and Interpretation 6, Accounting for Imputed Intra-departmental Costs: An Interpretation of SFFAS 4."

Figure 38-Statement of Net Cost by Responsibility Segment Cost and Earned Revenues with the Public and Intragovernmental Entities

(thousands)

Lines of Business	With the Public	Intragovernmental	Intra-WCF Eliminations	FY 2021
Computing Services				
Gross Costs	$ 271,980	$ 927,446	$ -	$ 1,199,426
Less earned revenues	6	(1,076,876)	-	(1,076,870)
Net Costs	271,986	(149,430)	-	122,556
TSEAS				
Gross Costs	7,859,553	267,698	-	8,127,251
Less earned revenues	(12,854)	(7,958,759)	-	(7,971,613)
Net Costs	7,846,699	(7,691,061)	-	155,638
Component Level				
Gross Costs	(196,500)	(740,110)	(6,331)	(942,941)
Less earned revenues	-	936,610	6,331	942,941
Net Costs	(196,500)	196,500	-	-
Net Cost of Operations				
Gross Costs	7,935,033	455,035	(6,331)	8,383,736
Less Total Revenues	(12,848)	(8,099,025)	6,331	(8,105,542)
Total Net Costs	$ 7,922,185	$ (7,643,990)	$ -	$ 278,194

Lines of Business	With the Public	Intragovernmental	Intra-WCF Eliminations	FY 2020
Computing Services				
Gross Costs	$ 236,320	$ 873,075	$ -	$ 1,109,396
Less earned revenues	(7)	(987,137)	-	(987,144)
Net Costs	236,314	(114,062)	-	122,252
TSEAS				
Gross Costs	7,603,827	236,329	-	7,840,156
Less earned revenues	(8,450)	(7,509,084)	-	(7,517,534)
Net Costs	7,595,377	(7,272,755)	-	322,622
Component Level				
Gross Costs	(283,750)	(595,318)	-	(879,069)
Less earned revenues	(2,082)	879,069	-	876,986
Net Costs	(285,833)	283,750	-	(2,082)
Net Cost of Operations				
Gross Costs	7,556,397	514,086	-	8,070,483
Less Total Revenues	(10,539)	(7,617,152)	-	(7,627,692)
Total Net Costs	$ 7,545,858	$ (7,103,066)	$ -	$ 442,791

*Component level represents adjustments entered into the Defense Departmental Reporting System (DDRS) at the DISA consolidated level.

Note 23- Exchange Revenues

COVID-19 Impacts
Please see Note 42

The DISA WCF reports exchange revenues for earned inflows of resources. They arise from exchange transactions, which occur when each party to a transaction sacrifices value and receives value in return. Pricing policy for exchange revenue is derived from stabilized rates established to recover estimated operating expenses incurred for the applicable FY and to provide sufficient working capital for the acquisition of fixed assets as approved by the under secretary of defense (comptroller). Stabilized rates and unit prices are established at levels intended to equate estimated revenues to estimated costs. When gains or losses occur in prior fiscal years resulting from under or over applied stabilized rates and/or prices, those gains or losses are incorporated into a current year's stabilized rates. However, the estimated revenues may not equal estimated costs.

Note 24- Inter-Entity Costs

COVID-19 Impacts
Please see Note 42

Intragovernmental costs and revenue are related to transactions between two reporting entities within the federal government. Public costs and revenue are exchange transactions made between the DISA WCF and a nonfederal entity.

The following schedules supports the summary information presented in the SNC and discloses separately intragovernmental activity (transactions with other federal agencies) from transactions with the public.

Costs incurred through the procurement of goods and services from both public and other federal agency providers along with revenues earned from public and other federal customers is shown for each line of business. Costs incurred and revenue earned for DISA WCF programs that received and provided services to one another have been adjusted so it is not reflected in these totals. The DISA WCF's services are priced to recover the full cost of resources consumed to produce the service.

Figure 39-Inter-Entity Costs

(thousands)

Gross Program Costs (Note 21)	2021	2020
Gross Costs	$ 8,383,736	$ 8,070,483
Less: Earned Revenue	(8,105,542)	(7,627,691)
Net Cost of Operations	278,194	442,791
Information Technology Contracts	4,172,229	4,069,080
Enterprise License Agreements	720,838	639,398
Reimbursable Telecommunications Services	890,296	840,746
Telecommunications Contracts	748,176	725,828
Other Programs	1,852,197	1,795,431
Less: earned revenue	(8,105,542)	(7,627,691)
Net other program costs:	$ 278,194	$ 442,791

The accompanying notes are an integral part of these statements.

Disclosures Related to the Statement of Budgetary Resources

Note 27- Available Borrowing/Contract Authority, End of Period

COVID-19 Impacts

Please see Note 42

In accordance with FMR, Chapter 19, paragraph 190302.B, DISA WCF does not have any available borrowing/contract authority balance at the end of the fiscal year.

Note 28- Undelivered Orders at the End of the Period

COVID-19 Impacts

Please see Note 42

As of Sept. 30, 2021, DISA WCF's net amount of budgetary resources obligated for undelivered orders is $895.6 million.

Figure 40-Budgetary Resources Obligated for Undelivered Orders at the End of the Period

(thousands)

	2021	2020
1. Intragovernmental		
A. Unpaid	$ 14,050	$ 336,674
B. Prepaid/Advanced	-	841
C. Total Intragovernmental	14,050	337,515
2. Non-Federal		
A. Unpaid	881,136	1,815,837
B. Prepaid/Advanced	401	-
C. Total Non-Federal	881,537	1,815,837
3. Total Budgetary Resources Obligated for Undelivered Orders at the End of the Period	$ 895,587	$ 2,153,352

Note 30- Legal Arrangements Affecting the Use of Unobligated Balances

COVID-19 Impacts

Please see Note 42

The DISA WCF does not have any legal arrangements affecting the use of unobligated budget authority and has not received any permanent indefinite appropriations.

Note 38 - Reconciliation of Net Cost to Net Outlays

The Reconciliation of Net Cost to Net Outlays demonstrates the relationship between the DISA WCF Net Cost of Operations, stated on an accrual basis on the Statement of Net Cost, and Net Outlays, and reported on a budgetary basis on the Statement of Budgetary Resources. While budgetary and financial accounting are complementary, the reconciliation explains the inherent differences in timing and in the types of information between the two during the reporting period. The accrual basis of financial accounting is intended to provide a picture of the DISA WCF's operations and financial position, including information about costs arising from the consumption of assets and the incurrence of liabilities. Budgetary accounting reports on the management of resources and the use and receipt of cash by the DISA WCF's. Outlays are payments to liquidate an obligation, other than the repayment to the Treasury of debt principal.

Figure 41- Reconciliation of the Net Cost of Operations to Net Outlays

(thousands)

DISA WCF 2021	Intragovernmental	With the Public	Total
1. Net Cost of Operations (SNC)	$ (7,622,966)	$ 7,901,160	$ 278,194
Components of Net Cost Not Part of Net Outlays:			
2. Property, plant, and equipment, net changes	-	17,685	17,685
3. Property, plant, and equipment disposal & revaluation	-	-	-
4. Year-end credit reform subsidy re-estimates	-	-	-
5. Increase/(decrease) in assets:			
a. Accounts and taxes receivable, net	(89,282)	(606)	(89,888)
b. Loans receivable, net	-	-	-
c. Other assets	(841)	401	(440)
6. (Increase)/decrease in liabilities:			
a. Accounts Payable	1,605	(39,490)	(37,885)
b. Loans guarantee liability	-	-	-
c. Insurance and guarantee program liabilities	-	-	-
d. Environmental and disposal liabilities	-	-	-
e. Benefits due and payable	-	-	-
f. Federal employee benefits payable	-	(934)	(934)
g. Other liabilities	(401)	(5,769)	(6,170)
7. Other financing sources:			
Imputed cost			
a. Imputed Cost	(56,900)	-	(56,900)
b. Donated revenue	-	-	-
8. Total Components of Net Cost That are Not Part of Net Outlays	(145,819)	(28,713)	(174,532)
Components of Net Outlays That Are Not Part of Net Cost:			
9. Acquisition of capital assets	-	-	-
10. Investments	-	-	-
11. Inventories and related property	-	-	-
12. Debt	-	-	-
13. Other	-	-	-
14. Total Components of Net Outlays That Are Not Part of Net Cost	-	-	-
Miscellaneous Reconciling Items			
15. Eliminations between financing and non-financing	-	-	-
16. Distributed offsetting receipts	-	-	-
17. Other	(119,794)	-	(119,794)
18. Total Other Reconciling Items	(119,794)	-	(119,794)

DISA WCF 2021	Intragovernmental	With the Public	Total
19. Total Net Outlays	$ (7,888,579)	$ 7,872,447	$ (16,131)
20. Agency Outlays, Net, Statement of Budgetary Resources			(16,131)
21. Unreconciled difference			$ -

Note 39- Public-Private Partnerships

The DISA WCF does not have Public, Private, Partnerships as defined by SFFAS 49. Subject to Definitional Features Indicative of Risk, Risk-based Characteristics, and Materiality (SFFAS 49, par 15) and for the purposes of this SFFAS 49, federal public-private partnerships (P3s) are risk-sharing arrangements or transactions with expected lives greater than five years between public and private sector entities. Such arrangements or transactions provide a service or an asset for government and/or general public use. In addition to the sharing of resources, each party shares in the risks and rewards of said arrangements or transactions.

Note 42-COVID-19 Activity

The DISA WCF did not use a significant amount of their FY 2021 budgetary resources to prevent, prepare for, or respond to COVID-19.

Note 45. Reclassification of Financial Statement Line Items for Financial Report Compilation Process.

COVID-19 Impacts

Please see Note 42

The Statement of Changes in Net Position (SCNP) reports the change in net position for the period, which results from changes to cumulative results of operations. During FY 2021, changes for the DISA WCF primarily consists of budgetary financing sources – other for transfers-in/out and along with the net cost of operations.

The DISA WCF does not have funds from dedicated collections and did not receive any supplemental appropriations during FY 2021.

These Notes Do Not Apply to the DISA WCF:

Note 4- Cash and Other Monetary Assets

Note 5- Investments

Note 7- Taxes Receivable, Net

Note 8- Loans Receivable, Net and Loan Guarantee Liabilities

Note 9- Inventory and Related Property, Net

Note 11- Stewardship PP&E

Note 14- Federal Debt and Interest Payable

Note 16- Environmental and Disposal Liabilities

Note 20- Funds from Dedicated Collections

Note 22- Stewardship PP&E Obtained Through Transfer, Donation or Devise

Note 25- Net Adjustments to Unobligated Balance, Brought Forward, Oct. 1

Note 26- Terms of Borrowing Authority Used

Note 29- Permanent Indefinite Appropriations

Note 31- Explanation of Differences between the SBR and the Budget of the U.S. Government

Note 32- Contributed Capital

Note 33- Incidental Custodial Collections

Note 34- Custodial Revenues

Note 35- Statement of Social Insurance and Statement of Changes in Social Insurance Amounts

Note 36- Fiduciary Activities

Note 37- Restatements

Note 40- Disclosure Entities and Related Parties

Note 41- Insurance Programs

Note 43- Subsequent Events

Note 44- Non-Custodial Non-Exchange Revenues

Required Supplementary Information

1. Deferred Maintenance and Repairs Disclosures

In accordance with FASAB SFFAS 42 and FMR 6B, Chapter 12, paragraph 120301, DISA is to report material amounts of deferred maintenance and repairs (DM&R) on its financial statements. DISA has not identified WCF DM&R in fiscal year 2021 to report. This determination is made based on existing contracts in place for current funded maintenance. Regularly scheduled maintenance on a continued basis eliminates a need for deferred maintenance. DISA preventative maintenance guidance and procedures are in place and address scheduled or unscheduled incidents requiring maintenance. DISA reviewed its facilities, hardware, and software to deter operational and security issues under current funding. There is no request for WCF funding for deferred maintenance. However, hardware programs are at risk if current maintenance is not in place. Further, a lack of software maintenance could pose a security threat in the DISA environment. Based upon these overarching considerations, preventative maintenance takes place with current contracts to ensure operational and security capabilities. Due to the nature of the DISA mission, required maintenance is not deferred and not ranked or prioritized among other activities. In addition, as of FY 2021, all real property has been transferred out of the DISA WCF.

For FY 2021, deferred maintenance reporting continues to be reviewed and revised as needed. The WCF does not have DM&R related to capitalized general PP&E, stewardship PP&E, non-capitalized or fully depreciated general PP&E. In addition, the DISA WCF does not have PP&E for which management does not measure and/or report DM&R. The rationale for excluding any PP&E asset other than if not capitalized or it is fully depreciated, is the item does not meet the applicable capitalization criteria, is not on the integrated project list, or there are preventative maintenance contracts in place to address maintenance needs in the current year.

No significant changes in policy, identification, or treatment of DM&R have occurred since the last FY.

Department of Defense
Defense Information Systems Agency WCF
As of Sept. 30, 2021
($ in thousands)

Figure 42-Balance Sheet Information

	CS	TSEAS	Combined	Intra-Entity Eliminations	FY 2021
Assets					
Intragovernmental:					
Fund Balance with Treasury	$ 31,709	$ 181,944	$ 213,653	$ -	$ 213,653
Accounts Receivable	98,663	893,440	992,104	(97,700)	894,403
Total Intragovernmental Assets	130,372	1,075,384	1,205,757	(97,700)	1,108,056
Other than intragovernmental:					
Accounts receivable, net	112	878	989	-	990
General PP&E, net	211,417	696,871	908,288	-	908,288
Advances and prepayments	-	401	401	-	401
Total other than intragovernmental	211,529	698,150	909,678	-	909,679
Total Assets	341,901	1,773,534	2,115,435	(97,700)	2,017,735
Liabilities					
Intragovernmental:					
Accounts payable	96,836	16,152	112,987	(89,127)	23,860
Other Liabilities	3,300	2,632	5,932	-	5,932
Total intragovernmental Liabilities	100,135	18,784	118,919	(89,127)	29,792
Other than intragovernmental liabilities:					
Accounts payable	23	959,027	959,050	(8,573)	950,477
Federal employee and Veteran Benefits Payable	3,041	2,971	6,011	-	6,012
Other Liabilities	31,162	26,379	57,541	-	57,541
Total other than intragovernmental	34,226	988,377	1,022,603	(8,573)	1,014,030
Total liabilities	134,361	1,007,161	1,141,522	(97,700)	1,043,822
Net Position:					
Cumulative Results of Operations – Funds Other than Dedicated Collections	207,540	766,373	973,913	-	973,913
Total net position	207,540	766,373	973,913	-	973,913
Total liabilities and net position	$ 341,901	$1,773,534	$ 2,115,435	$ (97,700)	$2,017,735

*The accompanying notes are an integral part of these statements.

Defense Information Systems Agency
Working Capital Fund
As of Sept. 30, 2021
(thousands)

Figure 43-Combining Statement of Budgetary Resources

	CS	TSEAS	Intra-Entity Eliminations	FY 2021
Budgetary Resources (discretionary and mandatory):				
Unobligated balance from prior year budget authority, net	$ 84,085	$ 275,692	$ (799)	$ 358,978
Contract Authority (discretionary and mandatory)	25,995	109,324	-	135,319
Spending Authority from offsetting collections	899,880	6,747,681	(1,183,606)	6,463,955
Total Budgetary Resources	1,009,960	7,132,697	(1,184,405)	6,958,252
Status of Budgetary Resources:				
New obligations and upward adjustments (total)	332,733	7,681,802	(1,154,647)	6,859,888
Unobligated balance, end of year: Apportioned, unexpired accounts	677,228	(549,105)	(29,759)	98,364
Unexpired unobligated balance, end of year	677,228	(549,105)	(29,759)	98,364
Unobligated balance, end of year (total)	677,228	(549,105)	(29,759)	98,364
Total Budgetary Resources	1,009,961	7,132,697	(1,184,406)	6,958,252
Outlays, net:				
Outlays, net (total) (discretionary and mandatory)	(547,418)	531,287	-	(16,131)
Agency Outlays, net (discretionary and mandatory)	$ (547,418)	$ 531,287	$ -	$ (16,131)

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2021
($ in thousands)

Figure 44- Statement of Net Cost

Program Costs	CS	TSEAS	Combined	Intra-Entity Eliminations	FY 2021
Gross Costs	$ 1,199,426	$ 8,127,251	$9,326,677	$ (942,941)	$ 8,383,736
Less: Earned Revenue	(1,076,870)	(7,971,613)	(9,048,483)	942,941	(8,105,542)
Net Cost of Operations	$ 122,556	$ 155,638	$ 278,194	$ -	$ 278,194

Other Information

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

08 October 2021

MEMORANDUM FOR DIRECTOR (D)

SUBJECT: Top Management and Performance Challenges Facing the Defense InformationSystems Agency (DISA) in Fiscal Year 2022

The Reports Consolidation Act of 2000 requires the DISA Office of the Inspector General (OIG) to issue a report summarizing what the OIG considers as serious management andperformance challenges facing DISA and assessing the Agency's progress in addressing those challenges. DISA is required to include this report in its agency financial report. This report represents DISA OIG's independent assessment of the top management challenges facing DISA in fiscal year 2022.

In developing this report, the DISA OIG considered several criteria including items suchas the impact on safety and cyber security, documented vulnerabilities, large dollar implications,high risk areas, and the ability of DISA to effect change. We reviewed recent and prior internal audits, evaluations, and investigation reports; reports published by other oversight bodies; and input received from DISA senior leadership. In addition, we recognize that DISA faces the extraordinary task of meeting these challenges while also responding to the Coronavirus Disease2019 (COVID-19) global pandemic and continuing to work in a maximum telework environment.

The DISA OIG identified five challenges this year. The challenges are not listed in a specific order and all are considered to be significant to DISA's work. DISA's Top Managementand Performance Challenges for Fiscal Year 2022 include:

- Meeting the 2020 DoD Data Strategy
- Managing Human Capital in a Post COVID-19 Environment
- Cyber Supply Chain Risk Management
- Current and Future Contracting Environment
- Mission Partner Payments

RYAN.STEPHEN.M ICHAEL [redacted] Digitally signed by RYAN.STEPHEN.MICHAEL [redacted] Date: 2021.10.08 10:13:48 -04'00'

Stephen M. Ryan
DISA Inspector General

Challenge 1
Meeting the 2020 DoD Data Strategy

DISA faces the challenge of meeting the DoD's data management goals outlined in the 2020 DoD Data Strategy. Data management is the practice of collecting, keeping, and using datasecurely. DISA has a vast infrastructure that transports mission partner data internally and externally while successfully maintaining various operating systems that produce massive amounts of complex data. Specifically, DISA must secure data and make it visible, accessible, and usable for analytics.

Per the DoD Strategy Memorandum, data security is an area the DoD must mature. The federal government is under constant data-driven cyber-attacks. For example, in June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting personnel records. Recently, in 2020, the 'Solar Winds' cyberattack by a groupbacked by a foreign government penetrated thousands of organizations globally including multiple parts of the United States federal government, leading to a series of data hacks. DISA has the responsibility to help DoD modernize the infrastructure and identify, protect, detect, respond, and recover from data threats.

The DoD Data Strategy also aims to evolve data into actionable information for decision makers.To help address these challenges, DISA established the Chief Data Officer (CDO). DISA is also re-aligning its policies, processes, and organizational structure to support enterprise data management. DISA is creating a data centric organization that uses data at speed and scale for operational advantage requiring DISA to fully understand the universe of operating systems and how that data is being used and where it is being stored. Investing in automation and a robust infrastructure that promotes sharing data across multiple platforms will allow DISA to breakdown current data silos.

Challenge 2
Managing Human Capital in a Post COVID-19 Environment

COVID-19 forced DISA to change the way it operates to accomplish its mission through maximum telework and new technologies and tools enhancing communication, collaboration, and coordination both internally and with mission partners. The rapidly changing environmentpresents new challenges on a daily basis requiring DISA leadership to adapt quickly. Moving forward, DISA leadership will be presented with new challenges in managing the new environment such as maintaining employee morale, managing and enhancing employee retention, on-boarding new employees, providing a safe and secure work environment, and embracing technology and tools while maintaining a strong culture and high productivity.

Employee morale and productivity in the evolving environment is part of the ongoing challenges.During evaluations conducted by the DISA OIG, the vast majority of interviewees said morale was the same or improved and pre-COVID productivity levels and quality of work were maintained. SES personnel interviewed indicated difficulty with determining metrics for measuring productivity in a virtual environment. Moving forward, morale and productivity may be impacted which can aid in shaping policies and identifying key metrics for monitoring performance and productivity. This challenge will present pros and cons of new policies including expanded telework and remote work as it relates to employee morale and productivity.

The evolving work environment that includes telework and remote work will require continuing assessment to maximize staffing and broaden the hiring pool of candidates in various geographical regions to attract and retain high quality talent. Identifying a clear vision of DISA's post-COVID-19 environment assists in recruiting and hiring highly qualified talent and retaining employees as more flexible options are considered a benefit. In addition, DISA will bechallenged to balance organizational needs with a sustainable number of employee positions to include manpower right-sizing efforts while retaining high quality staff.

Human capital improvements include the updates to how DISA on-boards new employees and physically protect employees. Conducting on-boarding virtually introduces new challenges with acclimating new employees into the DISA culture. A DISA OIG evaluation recommended extending the on-boarding and orientation time period to allow valued aspects of culture to be developed. DISA's workspace management decisions will be impacted by the need to protect employees through telework and social distancing creating additional challenges.

Technology is an important component in the virtual environment. As the Agency transitions, communication and collaboration through technology and other tools will be key to assist in managing all challenges of human capital.

Challenge 3
Cyber Supply Chain Risk Management

Strengthening and securing DISA's Cyber Supply Chain is an enduring management challenge. DISA provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to the warfighter,national-level leaders, Combatant Commands, and coalition partners across the full spectrum of military operations.

Cyber supply chain risk is the possibility an adversary may exploit the supply chain to corrupt our software, steal information, and carry out other malicious activities. To support this mission,DISA relies on an international supply chain to provide software, hardware, and services. The cyber supply chain includes a complex web of manufacturers, suppliers, and contractors.

To secure the cyber supply chain, DISA must protect, detect, respond, and recover from supply chain threats. Specifically, Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnectednature of Information Technology (IT) services and supply chains. C-SCRM covers the entire life cycle of the supply chain, including design, development, distribution, deployment, acquisition, maintenance, and destruction. C-SCRM also includes cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain. Successful C-SCRM maintains the integrity of products, services, people, technologies, and ensures the undisrupted flow of product, materiel, information, and finances.

Examples of DISA Cyber Supply Chain risks include mobile technology, commercial off the shelf (COTS) technology, and reliance of foreign suppliers. Fifth generation wireless technology, more commonly called 5G, builds upon existing telecommunication infrastructure toimprove bandwidth and capabilities and reduce network-generated delays. The 5G networks may introduce vulnerabilities such as malicious software and hardware, counterfeit components, and interconnectivity of foreign equipment. Similarly, COTS software and hardware allows DISA to adopt current and effective technologies and are integrated into existing IT systems, butoften these supplies come from foreign suppliers which increases the risk to DISA systems.
Ultimately, DISA and the Department will face a significant challenge safeguarding the cybersupply chain as well as finding domestic supply sources

Challenge 4
Current and Future Contracting Environment

Contracting is a top management challenge at DISA due to increased mission partner contracting requirements without the respective increase in staffing levels causing the inability to sufficientlyand effectively meet DoD and other federal agency mission needs. DISA Procurement Services Directorate (PSD)/Defense Information Technology Contracting Organization (DITCO) providesprocurement services for Information Technology, Telecommunications, and Cyber domains in defense of our nation. PSD has turned away mission partner requests in the past year, resulting in lost revenue, due to DISA's hiring limitations and PSD's mission requirements, increasing workload, and retention challenges.

In addition, PSD identified the submission of late procurement packages and late funding from internal and external mission partners as a challenge. Late procurement packages occurred because of contract package routing delays, requirement definition issues, unfunded requirements delays, and contract scope issues. Other challenges in contracting faced by PSD and mission partners are increased by OMB, OSD, DoD, and DISA funding and other indirect process issues. PSD and the Office of the Chief Financial Officer are collaborating to implementprocess improvements to fulfill contract requirements in a timely manner and meet mission partner needs.

The DISA Office of Inspector General (OIG) audits also reported concerns relating to contracting at DISA; specifically, contracts pertaining to mobility devices, government furnishedproperty, cyber safeguards of defense information clause, and contractor workspace designations. Additionally, evaluations reported concerns relating to Contracting Officer Representative (COR) performing their duties and DITCO's oversight of CORs. CORs ensure delivery of supplies and critical mission services; however, inadequate COR oversight could result in a decreased quality of contractor services.

Challenge 5
Mission Partner Payments

DISA continues to have challenges obtaining Mission Partner (Military Services and Defense/Non-Defense Agencies) payments in a timely manner for reimbursable costs incurred. DISA provides goods and services through the Defense Working Capital Fund (DWCF) Computing and Telecommunications process or by appropriated reimbursable economy act orders. The goal of this reimbursable support is for customers to leverage the buying power of the Government to acquire goods and services in the most efficient and cost-effective manner. DISA DWCF in FY21 managed approximately 2,534 Computing orders, 16,323 PDCs, and 526 Telecommunication MIPRs. DISA General Fund managed 1,588 reimbursable projects.

DISA spends a considerable amount of staffing resources and time reaching out to Mission Partners on delinquent account receivables (AR) for reimbursable orders. DISA officials take several actions to attempt collection of past due accounts by holding several meetings with Mission Partners throughout the year to discuss the respective past due AR, sending notices when each AR reaches 90-days delinquent, and issuing formal collection letters when each AR reaches 120-days delinquent. Finally, if a Mission Partner is not reimbursing DISA according to the support agreement for services previously ordered, the OCFO elevates to the Under Secretary of Defense (C) (PB) and/or Treasury for further collection action. This challenge is compounded by multiple factors outside of DISA's control. According to DISA OCFO, there were numerous reasons why Mission Partners are waiting to submit payment closer to the fiscal year end to include: funding uncertainties, reduced budgets, changes to Reimbursable Agreements, and no penalties applied to customers with delinquent accounts. Delaying payment increases DISA's risk of not collecting payment by fiscal year end. The total past due accounts receivable at 30 Sept. 2021, totaled $6.79M in Computing and $2.64M in Telecommunications DWCF orders. The total past due accounts receivable for the DISA General Funds at Sept. 30, 2021, totaled $10.5M.

OFFICE OF THE INSPECTOR GENERAL

The Office of the Inspector General (OIG) is an impartial fact-finder for the Director and leaders of DISA. The OIG seeks to improve the efficiency and effectiveness of DISA's programs and operations by conducting Audits, Investigations, and Evaluations. The OIG then evaluates and coordinates to close the recommendations through the Liaison office.

AUDIT

OIG Audit provides independent and objective audit services to promote continuous performance improvement, management, and accountability of DISA operations, programs, and resources to support DISA's missions as a Combat Support Agency. The types of services OIG Audit providesare performance audits, attestation engagements, financial audits, and, occasionally, non-audit services. OIG Audit is built on a framework for performing high-quality audit work with competence, integrity, and transparency.

INVESTIGATION

OIG Investigation supports the efficiency and effectiveness of DISA by providing accurate, thorough, and timely investigative products to key Agency leaders. OIG Investigation performs five primary functions: Hotline Program, Administrative Investigations, Digital Forensics, Criminal Investigation Liaison Support, and Fraud Awareness Program. Fundamental purpose of investigations is to resolve specific allegations, complaints, or information concerning possible violations of law, regulation, or policy.

EVALUATION

OIG Evaluation conducts evaluations and special inquiries to improve processes, optimize the effective use of military and civilian personnel, enhance operational readiness, assess focus areas, and provide recommendations for improvement while teaching and training. The fundamental purpose of evaluations is to assess, assist, and enhance the ability of a command or component toprepare for and perform its assigned mission.

LIAISON

OIG Liaison serves as the conduit between DISA and external parties by providing guidance and assistance ensuring leadership, at all levels, is appropriately informed and ensuring external agency objectives are met while minimizing the impact to DISA operations. OIG Liaison supports DISA as a whole by providing:

- Audit Coordination- Monitor all oversight activities impacting DISA.
- Communication- Liaison between DISA leadership and external parties.
- Follow-up- Track and ensure implementation of all external/internal recommendations.

Summary of Financial Statement Audit and Management Assurances
Audit Opinion: Unmodified
Restatement: No

Figure 45-Summary of Financial Statement Audit

Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Ending Balance
	0	0	0	0	0
	0	0	0	0	0
Total Material Weaknesses	0	0	0	0	0

Figure 46-Effectiveness of Internal Control over Financial Reporting (FMFIA§ 2)
Statement of Assurance: Unmodified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Categories:						
Fund Balance with Treasury	5	0	0	0	0	5
Accounts Payable/Expense	6	1	-2	0	0	5
Accounts Receivable/Revenue	2	0	0	0	0	2
Internal Controls	1	0	0	0	-1	1
Unmatched Transactions	1	0	0	0	-1	1
Financial Reporting	2	1	-1	0	-1	1
Undelivered Orders	2	0	0	0	0	2
Unfilled Customer Orders	1	0	0	0	0	1
Total Material Weaknesses	20	2	-3	0	-3	18

Figure 47-Effectiveness of Internal Control over Operations (FMFIA§ 2)
Statement of Assurance: Unmodified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Total Material Weaknesses	0	0	0	0	0	0

Figure 48- Conformance with Federal Financial Management System Requirements (FMFIA**§ 4)**
Statement of Assurance: Unmodified

Non-Conformances	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
IT-Related	7	3	-4	0	0	6
Total non-conformance	7	3	-4	0	0	6

Figure 49-Compliance with Section 803(a) of the Federal Financial Management Improvement Act (FFMIA)

Compliance Objective	Agency	Auditor
Federal Financial Management System Requirements	No lack of compliance noted except as noted in IT related material weaknesses above	No lack of compliance noted
Applicable Federal Accounting Standards	No lack of compliance noted except as noted in financial reporting related material weaknesses above	No lack of compliance noted
USSGL at Transaction Level	No lack of compliance noted	No lack of compliance noted

Payment Integrity

For compliance with the Payment Integrity Information act of 2019 (Pub. L. No. 116-117, 31 U.S.C. § 3352 and § 3357), DISA has an internal control structure in place to mitigate improper payments that could result in payment recovery actions. Actions taken to prevent overpayments include testing and review of civilian time and attendance, travel payments, and purchase card transactions. Tests validate that internal controls are in place and functioning as preventative measures to mitigate risks in the execution, obligation, and liquidation of funding for transactions. Controls are in place through established policy and procedures; training; separation of duties; and data mining to identify risks and fraud vulnerabilities. Additionally, the Defense Finance and Accounting Service (DFAS), as DISA's accounting service provider, performs overpayment recapture functions on behalf of DISA. DFAS includes DISA transactions in their sampling populations for improper payment testing.

DoD Office of the Inspector General Audit Report Transmittal Letter

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

December 16, 2021

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
CHIEF FINANCIAL OFFICER, DOD
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Transmittal of the Independent Auditor's Reports on the Defense Information Systems Agency Working Capital Fund Financial Statements and Related Notes for FY 2021 and FY 2020 (Project No. D2021-D000FL-0066.000, Report No. DODIG-2022-044)

We contracted with the independent public accounting firm of Kearney & Company to audit the Defense Information Systems Agency (DISA) Working Capital Fund Financial Statements and related notes as of and for the fiscal years ended September 30, 2021, and 2020. The contract required Kearney & Company to provide a report on internal control over financial reporting and compliance with provisions of applicable laws and regulations, contracts, and grant agreements, and to report on whether DISA's financial management systems substantially complied with the requirements of the Federal Financial Management Improvement Act of 1996. The contract required Kearney & Company to conduct the audit in accordance with generally accepted government auditing standards (GAGAS); Office of Management and Budget audit guidance; and the Government Accountability Office/Council of the Inspectors General on Integrity and Efficiency, "Financial Audit Manual," June 2018, Volume 1 (Updated, April 2020), Volume 2 (Updated, March 2021), and Volume 3 (Updated, September 2021). Kearney & Company's Independent Auditor's Reports are attached.

Kearney & Company's audit resulted in an unmodified opinion. Kearney & Company concluded that the DISA Working Capital Fund Financial Statements and related notes as of and for the fiscal years ended September 30, 2021, and 2020, are presented fairly, in all material aspects, in conformity with Generally Accepted Accounting Principles.

Kearney & Company's separate report, "Independent Auditor's Report on Internal Control Over Financial Reporting," discusses three material weaknesses related to the

DISA Working Capital Fund's internal controls over financial reporting.* Specifically, Kearney & Company's report concluded that DISA did not implement adequate controls to:

- reconcile and report Fund Balance With Treasury;
- validate, reconcile, and support Accounts Receivable, revenue, Accounts Payable, and expense transactions; and
- analyze and record budgetary resource related transactions.

Kearney & Company's additional report, "Independent Auditor's Report on Compliance With Laws, Regulations, Contracts, and Grant Agreements," discusses two instances of noncompliance with provisions of applicable laws and regulations, contracts, and grant agreements. Specifically, Kearney & Company's report describes instances in which DISA did not comply with the Federal Managers' Financial Integrity Act of 1982 and the Prompt Payment Act of 1982.

In connection with the contract, we reviewed Kearney & Company's reports and related documentation and discussed them with Kearney & Company's representatives. Our review, as differentiated from an audit of the financial statements and related notes in accordance with GAGAS, was not intended to enable us to express, and we do not express, an opinion on the DISA Working Capital Fund FY 2021 and FY 2020 Financial Statements and related notes. Furthermore, we do not express conclusions on the effectiveness of internal control over financial reporting, on whether DISA's financial systems substantially complied with Federal Financial Management Improvement Act of 1996 requirements, or on compliance with provisions of applicable laws and regulations, contracts, and grant agreements. Our review disclosed no instances where Kearney & Company did not comply, in all material respects, with GAGAS. Kearney & Company is responsible for the attached December 16, 2021 reports, and the conclusions expressed within the reports.

* A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting that results in a reasonable possibility that management will not prevent, or detect and correct, a material misstatement in the financial statements in a timely manner.

We appreciate the cooperation and assistance received during the audit. Please direct questions to me.

Lorin T. Venable, CPA
Assistant Inspector General for Audit
Financial Management and Reporting

Attachments:
As stated

Independent Auditor's Report

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

INDEPENDENT AUDITOR'S REPORT

To the Director, Defense Information Systems Agency, and Inspector General of the Departmentof Defense

I. Report on the Financial Statements

We have audited the accompanying Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency (DISA), which comprise the balance sheets as of September 30, 2021 and 2020, the related statements of net cost and changes in net position, andthe combined statements of budgetary resources (hereinafter referred to as the "financial statements") for the years then ended, and the related notes to the financial statements.

II. Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statementsin accordance with accounting principles generally accepted in the United States of America; thisincludes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement,whether due to fraud or error.

III. Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government AuditingStandards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 21-04, *Audit Requirements for Federal Financial Statements*.
Those standards and OMB Bulletin No. 21-04 require that we plan and perform the audit toobtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financialstatements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control.
Accordingly, we express no such opinion. An audit also includes evaluating the appropriatenessof accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide abasis for our audit opinion.

IV. Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects,the financial position of the DISA WCF as of September 30, 2021 and 2020, and its net cost ofoperations, changes in net position, and budgetary resources for the years then ended, in accordance with accounting principles generally accepted in the United States of America.

V. Other Matters

A. Required Supplementary Information

Accounting principles generally accepted in the United States of America require that Management's Discussion and Analysis (hereinafter referred to as the "required supplementary information") be presented to supplement the financial statements. Such information, although not a part of the financial statements, is required by OMB and the Federal Accounting StandardsAdvisory Board (FASAB), who consider it to be an essential part of financial reporting for placing the financial statements in an appropriate operational, economic, or historical context.
We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management regarding the methods of preparing the information and comparing it for consistency with management's responses to our inquiries, the financial statements, and other knowledge we obtained during our audits of the financial statements. Wedo not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

B. Other Information

Our audits were conducted for the purpose of forming an opinion on the financial statements taken as a whole. Other Information, as named in the Agency Financial Report (AFR), is presented for purposes of additional analysis and is not a required part of the financial statements. Such information has not been subjected to the auditing procedures applied in theaudits of the financial statements; accordingly, we do not express an opinion or provide any assurance on it.

KEARNEY& COMPANY

C. Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards* and OMB Bulletin No. 21-04, we have alsoissued reports, dated December 16, 2021, on our consideration of the DISA WCF's internal control over financial reporting and on our tests of the DISA WCF's compliance with provisionsof applicable laws, regulations, contracts, and grant agreements, as well as other matters for the year ended September 30, 2021. The purpose of those reports is to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing,and not to provide an opinion on internal control over financial reporting or on compliance and other matters. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 21-04 and should be considered in assessing the results of our audits.

Alexandria, Virginia
December 16, 2021

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

To the Director, Defense Information Systems Agency, and Inspector General of the Departmentof Defense

We have audited, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 21-04, *Audit Requirements for Federal Financial Statements*, the Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency (DISA) as of and for the year ended September 30, 2021, and the related notes to the financial statements, which collectively comprise the DISA WCF's financial statements, and wehave issued our report thereon dated December 16, 2021.

I. Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered the DISA WCF's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the DISA WCF's internal control. Accordingly, we do not express an opinion on the effectiveness of the DISA WCF's internal control. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 21-04. We didnot test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA), such as those controls relevant to ensuring efficient operations.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies; therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanyingSchedule of Findings, we did identify certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented,or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings to be material weaknesses.

KEARNEY& COMPANY

A significant deficiency is a deficiency, or combination of deficiencies, in internal control that isless severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying Schedule of Findings to be significant deficiencies.

We noted certain additional matters involving internal control over financial reporting that wewill report to the DISA WCF's management in a separate letter.

II. DISA's Response to Findings

The DISA WCF's response to the findings identified in our audit is described in a separate memorandum attached to this report of the Agency Financial Report (AFR). The DISA WCF'sresponse was not subjected to the auditing procedures applied in the audit of the financial statements; accordingly, we express no opinion on it.

III. Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and theresults of that testing, and not to provide an opinion on the effectiveness of the DISA WCF's internal control. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 21-04 in considering the entity's internalcontrol. Accordingly, this communication is not suitable for any other purpose

Alexandria, Virginia
December 16, 2021

KEARNEY& COMPANY

Schedule of Findings

Material Weaknesses

Throughout the course of our audit work at the Defense Information Systems Agency (DISA), we identified internal control deficiencies which were considered for the purposes of reporting on internal control over financial reporting. The material weaknesses presented in this Scheduleof Findings have been formulated based on our determination of how individual control deficiencies, in aggregate, affect internal control over financial reporting. ***Exhibit 1*** presents thematerial weaknesses identified during our audit.

Exhibit 1: Material Weaknesses and Sub-Categories

Material Weakness	Material Weakness Sub-Category
I. Fund Balance with Treasury	A. Budget Clearing Account Reconciliation and Reporting Processes B. Statement of Differences Reconciliation and Reporting Processes C. Lack of Controls over the Department 97 Reconciliation and Reporting Tool Process
II. Accounts Receivable/ Revenue and Accounts Payable/Expense	A. Allowance for Doubtful Accounts B. Unmatched Transactions and Lack of Collection Validations C. Lack of Accounts Payable/Expense Accrual Validation D. Lack of Receipt and Acceptance E. Lack of Operating Effectiveness Relating to the Certification and Documentation of Travel Expense
III. Budgetary Resources	A. Lack of Lookback Analysis over Dormant Control B. Untimely Undelivered Order Transactions

I. Fund Balance with Treasury *(Repeat Condition)*

Deficiencies in three related areas, in aggregate, define this material weakness:

A. Budget Clearing Account Reconciliation and Reporting Processes
B. Statement of Differences Reconciliation and Reporting Processes
C. Lack of Controls over the Department 97 Reconciliation and Reporting Tool Process

A. Budget Clearing Account Reconciliation and Reporting Processes

Background: DISA uses a service organization to manage, report, and account for Fund Balancewith Treasury (FBWT) budget clearing (suspense) account activities to the U.S. Department of the Treasury (Treasury). DISA is responsible for monitoring and approving the FBWT reconciliations performed by its service organization on its behalf and is responsible for the complete and accurate reporting of FBWT on its financial statements and disclosures.

Budget clearing accounts temporarily hold unidentifiable general, revolving, special, or trust fund collections or disbursements that belong to the Federal Government. An "F" preceding thelast four digits of the fund account symbol identifies these funds. These clearing accounts are tobe used only when there is a reasonable basis or evidence that the collections or disbursements belong to the U.S. Government and, therefore, properly affect the budgetary resources of the Department of Defense (DoD) activity. None of the collections recorded in clearing fund accounts are available for obligation or expenditure while in a clearing account. Agencies should have a process to research and properly record clearing account transactions in their general ledger (GL) timely. The Treasury Financial Manual (TFM) Bulletin No. 2021-03, *Reporting Suspense Account Activity Using F3875 and F3885 and Using Default Accounts F3500 and F3502 as a Central Accounting Reporting System (CARS) Reporter*, requires that transactions be researched and properly cleared from the accounts within 60 days.

DISA suspense transactions, if any, are included and accounted for in the Treasury Index (TI) 97Other Defense Organizations (ODO), the Department of the Navy (TI-17), the Department of theAir Force (TI-57), and the Department of the Army (TI-21) suspense accounts, based on DoD disbursing processes.

Condition: DISA, in coordination with its service organization, has not implemented sufficient internal control activities to ensure that transactions recorded in suspense accounts do not containDISA collections and disbursements that should be recognized in the DISA accounting records. While its service organization prepares quarterly suspense management analyses for each TI to identify the total count and amount of suspense account transactions resolved to DISA and other Defense agencies, the management analyses are not available after quarter-end in a timely manner to perform sufficient analysis for financial reporting.

Cause: DISA's suspense activity is not recorded in unique suspense accounts, but rather in shared TI-97, TI-57, TI-21, and TI-17 suspense accounts. DoD suspense accounts continueto contain a high volume of collections and disbursements which require manual research and resolution. DISA and its service organization have not designed or implemented a methodology to determine the financial reporting impact of DoD suspense account balancesto DISA's financial statements for financial reporting.

Effect: DISA cannot identify or record its suspense activity into its GL and financial statements pursuant to quarterly financial reporting timelines. Without additional compensating internal controls or monitoring procedures and analyses, the lack of methodology to determine the financial reporting impact of the suspense balances inhibits DISA's ability to assert to the completeness and accuracy of reported FBWT on its BalanceSheet and other financial statement line items, as applicable.

Recommendations: Kearney & Company, P.C. (Kearney) recommends that DISA implementinternal control activities to ensure that material DISA transactions, individually and in the aggregate, are identified and appropriately included within DISA's accounting records.
Specifically, Kearney recommends that DISA perform the following:

1. Continue implementing business process improvements to prevent items from reaching suspense.
2. Research and resolve suspense transactions by correcting the transactions in source systems and assist its service organization with the necessary supporting documentation for corrections, if needed.
3. Consider any limitations to its service organization's suspense account reconciliation process and develop compensating controls to reconcile any included FBWT suspense activity or, through documented materiality analysis, indicate that management accepts the risk of potential misstatement.
4. Pursuant to receiving the necessary information and documentation from its service organization, develop and implement procedures to identify DISA's actual or estimated suspense account balances for recording and reporting into the GLs and financial statements. Estimates should only be developed using relevant, sufficient, and reliable information.
5. Work with its service organization to continue to develop procedures to determine what portion of the suspense balances, if any, should be attributed to DISA for financial reporting in a timely manner, available for year-end financial reporting purposes.
6. Work with its service organization to continue to monitor and track the resolution of suspense activity cleared to DISA to enable DISA to perform root cause analysis.
7. Work with its service organization to continue to work to implement more effective system and process controls to ensure that disbursements and collections are processed with valid TI, Treasury Account Symbol (TAS), and fiscal year (FY) inputs.
8. Work with its service organization to continue to develop and implement processes and controls to eliminate instances where transactions are being placed in suspense accounts intentionally.

B. Statement of Differences Reconciliation and Reporting Process

Background: DISA uses a service organization to provide daily Non-Treasury Disbursing Office (NTDO) disbursing services under various Agency Location Codes (ALC), often referredto as Disbursing Symbol Station Numbers (DSSN). Additionally, DISA's service organization provides monthly Treasury reporting services under various reporting ALCs, which are different than disbursing ALCs. Monthly, NTDO disbursing activity is submitted to its assigned reportingALC to generate a consolidated Standard Form (SF)-1219, *Statement of Accountability*, and SF- 1220, *Statement of Transactions*. Daily, Treasury Disbursing Office (TDO) ALCs submit reports directly to Treasury and complete SF-224, *Statement of Transactions*, at month-end.
DoD Components are responsible for investigating and resolving these differences and reportingany required adjustments on their monthly submissions to Treasury.

Treasury compares data submitted by financial institutions and Treasury Regional Financial Centers to ensure the integrity of the collection and disbursement activity submitted. A Statement of Differences (SOD) report, known as the Financial Management Services (FMS) 6652, is generated monthly in Treasury's CARS. The SOD report identifies discrepancies between the collections and disbursements reported to Treasury and what was actually processedfor each ALC by accounting month (i.e., the month the report is generated) and accomplished month. DISA is responsible for researching and resolving all differences identified on the FMS 6652 for its ALCs.

There are three categories of SOD reports generated by Treasury: 1) Deposit in Transit (DIT); 2)Intra-Governmental Payment and Collections (IPAC) or Disbursing; and 3) Check Issued.
Disbursing Officers responsible for applicable disbursing ALCs are required to research andresolve DIT, IPAC, and Check Issued differences monthly. DISA's service organization hasthree reporting ALCs, which are responsible for month-end reporting of collections and disbursements to Treasury.

Condition: DISA, in coordination with its service organization, has not implemented sufficientinternal control activities to ensure that transactions which comprise the SOD balances in DISA's primary DSSNs do not contain DISA collections and disbursements that should be recognized in DISA's accounting records. While its service organization prepares quarterly SOD management analyses for each DSSN to identify the total count and amount of SOD transactions resolved to DISA and other Defense agencies, the management analyses are not available after quarter-end in a timely manner to perform sufficient analysis for financial reporting.

Cause: The process performed by DISA's service organization to create the SOD UoTs is a time-intensive and manual process that requires the consolidation of multiple files from varioussources and subsequent manual research to identify the owners of the transactions. As such, theUoTs are not available after quarter-end in a timely manner to perform sufficient analysis for financial reporting and often do not identify the responsible reporting entity for each transaction. DISA and its service organization have not designed or implemented a methodology to determine the financial reporting impact of the SOD balances to DISA's financial statements. While its service organization has continued efforts to identify root causesby DSSN to reduce SOD balances and clear transactions to DoD entities timely, shared ALCs and lack of Line of Accounting (LOA) information continue to make it difficult to resolve differences timely.

Effect: DISA cannot identify and record its SOD activity into its GL and financial statements pursuant to quarterly financial reporting timelines. Without receiving the complete and final UoTs in a timelier manner, as well as additional compensating internal controls or monitoring procedures and analyses, the lack of methodology to determine the financial reporting impact ofthe SOD balances inhibits DISA's ability to assert to the completeness and accuracy of reportedFBWT on its Balance Sheet and other financial statement line items, as applicable.

Recommendations: Kearney recommends that DISA implement internal control activities toensure that material DISA transactions, individually and in the aggregate, are identified and appropriately included within the DISA's accounting records. Specifically, Kearney recommends that DISA perform the following:

1. Work with its service organization to coordinate and provide supporting information to clear transactions timely.
2. Continue working with Treasury, the Office of the Secretary of Defense (OSD), its service organization, and other parties to transition away from using monthly NTDO reporting ALCs to daily TDO reporting ALCs.
3. Consider any limitations to its service organization's SOD reconciliation process and develop compensating controls to reconcile any included FBWT SoD activity in an effort to minimize the risk of a potential material misstatement, or, through documented materiality analysis and risk assessment, indicate that management accepts the risk of potential misstatement.
4. Pursuant to receiving the necessary information and documentation from its service organization, develop and implement procedures to identify DISA's actual or estimated SOD balances for recording and reporting into the GLs and financial statements. Estimates should only be developed using relevant, sufficient, and reliable information.
5. Work with its service organization to continue to develop procedures to determine what portion of the SOD balances, if any, should be attributed to DISA for financial reporting in a timely manner, available for year-end financial reporting purposes.
6. Work with its service organization to continue to work towards researching and resolving SoD transactions in a timely manner.
7. Work with its service organization to continue assessing and identifying ALCs that primarily report collection and disbursement activity to Treasury on behalf of DISA.
8. Work with its service organization to continue to monitor and track the resolution of SODs cleared to DISA to enable DISA to perform root cause analysis and create projections of potential outstanding unresolved balances.
9. Continue scheduling recurring meetings with its service organization to help resolve outstanding differences.

C. Lack of Controls over the Department 97 Reconciliation and Reporting Tool Process

Background: DISA is a DoD agency that is required to prepare quarterly and annual financial statements in accordance with U.S. Generally Accepted Accounting Principles (GAAP), as established by the Federal Accounting Standards Advisory Board (FASAB).

The Department 97 Reconciliation and Reporting Tool (DRRT) is primarily used to reconcile TI97 ODO disbursements and collections that have posted to the Treasury against the detailed transactions recorded in the ODOs' GL systems, as well as provide the basis for agencies' undistributed adjustments journal vouchers (JV). DRRT is a Transact-Structured Query Language (SQL) programmed system developed by DISA's service organization.

DISA's service organization uses DRRT to perform monthly FBWT reconciliations for multiple ODOs, including DISA, to identify differences in FBWT balances between what is reported on the Cash Management Report (CMR) and what is recorded in an entity's GL system. Individual ODOs utilize various financial systems, and financial data from these are collectively imported into DRRT for processing at DISA's service organization. The DRRT reconciliation process exists to ensure that the net FBWT balance attributed to and reported within an ODO's GL, including DISA Working Capital Fund's (WCF) Financial Accounting Management InformationSystem (FAMIS-WCF) GL system, ties to the balance reported on the CMR for that agency.
DISA is responsible for reconciling its FBWT monthly and maintaining effective internal controls over its financial reporting to prevent or detect material misstatements in a timely manner. This includes coordinating with its service organization, as necessary, and monitoring,reviewing, and approving the reconciling procedures performed on their behalf. Without administering these steps, DISA is at risk of posting unsupported adjusting entries and potentially reporting material misstatements in its financial statements.

Condition: DISA does not validate the information received from DRRT or have front-end controls in place to confirm the accuracy and completeness of the data attributed to DISA WCF.

DISA's service organization does not have procedures or controls in place to reconcile input dataimported into DRRT back to original source systems. Additionally, DISA's service organizationdoes not have a process in place to validate that the limits assigned to transactions within DRRT are accurate and attributed to the correct entities, including the transactions attributed to DISA WCF.

Cause: DISA and its service organization did not design or implement effective FBWT reconciliation controls to ensure that accurate, complete, and properly supported financial data isincluded within the DRRT reconciliation. DISA does not have an effective Office of Management and Budget (OMB) Circular A-123 program or an enterprise risk assessment process in place, which would include developing detective controls over recurring financial reporting procedures. Additionally, DISA's internal control program does not include testing controls to ensure they address the applicable financial reporting objectives.

Effect: As a result of the lack of effective controls over the DRRT reconciliation process, FBWTmay be misstated and include transactions that do not belong to DISA, and misstatements may not be detected and corrected timely, causing a potential misstatement of DISA's financial statements.

Recommendations: Kearney recommends that DISA perform the following:

10. Develop and implement procedures for effective communication with its service organization management throughout the DRRT reconciliation process to ensure there is DISA management review and approval of the data being attributed to DISA from DRRT.

11. Develop and implement effective controls to ensure the validation and/or review of the data received its service organization, produced by DRRT, before it is recorded into DISA's GL system.
12. Coordinate with its service organization to develop and implement a process in which data imported into DRRT is traced to original source systems and the accuracy of the LOA information is validated.
13. Develop a more effective internal control program, including an enterprise-wide risk assessment, to determine risks in financial reporting and implement detective controls in line with financial reporting objectives.
14. Work with its service organization to develop and implement effective controls related to identifying and analyzing the risk with regard to the incorrect and incomplete data used for ODOs' financial statement compilation, including an analysis of internal and external factors, involving appropriate level of management, and determining how to respond to risk.
15. Work with its service organization to develop and implement effective procedures to internally communicate information necessary to support the functioning of internal controls related to the DRRT reconciliation, including relevant objectives and responsibilities. These procedures should include the flow of information up, down, and across the organization using a variety of methods and channels.

II. Accounts Receivable/Revenue and Accounts Payable/Expense *(Repeat Condition)*

Deficiencies in five related areas, in aggregate, define this material weakness:

A. Allowance for Doubtful Accounts
B. Unmatched Transactions and Lack of Collection Validations
C. Lack of Accounts Payable/Expense Accrual Validation
D. Lack of Receipt and Acceptance
E. Lack of Operating Effectiveness Relating to the Certification and Documentation of Travel Expense

A. Allowance for Doubtful Accounts

1. Lack of Implementation of Technical Bulletin 2020-1

Background: FASAB's Technical Bulletins provide guidance for agencies in order to properlyapply FASAB Statements and Interpretations, as well as resolve accounting issues not directly addressed by FASAB. Additionally, the following types of guidance may be provided within aTechnical Bulletin:

- Guidance to clarify, explain, or elaborate on an underlying Statement or Interpretation
- Guidance to address areas not directly covered by existing Statements or Interpretations
- Interim guidance on problems in applying an existing Statement or Interpretation currently under study by FASAB

- If applicable, guidance for applying Financial Accounting Standards Board (FASB) or Government Accounting Standards Board (GASB) standards to Federal activities.

FASAB issued Technical Bulletin 2020-1, *Loss Allowance for Intragovernmental Receivables*,on February 20, 2020 and required implementation upon issuance in FY 2020. Technical Bulletin 2020-1 documented that an allowance for estimated uncollectible amounts should be recognized in order to reduce the gross amount of receivables to its net realizable value. The allowance for uncollectible amounts should be re-estimated on each applicable annual financialreporting date, as well as when it would be applicable that the most recent estimate would no longer be accurate.

Condition: As of Quarter (Q) 2 of FY 2021, DISA WCF had not yet implemented the applicable provisions of FASAB Technical Bulletin 2020-1, which establishes the requirement to determineif a loss allowance is required relating to any outstanding intragovernmental receivables. DuringFY 2021, DISA created a policy regarding Technical Bulletin 2020-1. However, it did not document an analysis over the outstanding Aged Accounts Receivable (AR) balances in order to determine whether DISA would collect the receivables from its Federal agency customers and, therefore, if an allowance was required.

Cause: As of Q2 and during audit walkthroughs, DISA had not finalized its internal policy to monitor, execute, and consistently apply the methodology of the Technical Bulletin 2020-1- required implementation within the aged AR and Allowance for Doubtful Accounts. DISA did not document its assessment and determination on whether the WCF would apply the updates toits Intragovernmental AR outstanding balance. DISA's internal control program does not yet include a risk assessment that links risks to financial statement lines or assertions. It also does not include testing controls to ensure they address the applicable financial reporting objectives. Updates to the internal control program will help to identify and remediate control gaps.

Effect: Without procedures and a documented analysis to implement, determine, and apply Technical Bulletin 2020-1 on DISA's AR balances, specifically that of the IntragovernmentalReceivables, included on its Balance Sheet are at increased risk for misstatements.

Recommendations: Kearney recommends that DISA perform the following:

1. Perform and document an assessment to determine if an allowance for doubtful accounts, including those from Federal entities, is required per Technical Bulletin 2020-1.
2. Update the policies and Standard Operating Procedures (SOP) to reflect any changes or processes created to document DISA management's assessment.

2. **Untimely Implementation of Controls and Treasury Report on ReceivablesApprovals**

Background: Treasury requires each reporting entity to prepare a quarterly Treasury Report on Receivables (TROR). The TROR serves as a management report that informs Federal decision-makers of the gross book value of the receivables owed to Federal agencies and the status of theFederal Government's debt portfolio. On a monthly basis, agencies also create the Monthly Receivables Data (MRD) Report, which outlines the monthly amounts of the receivables noted that are essentially combined quarterly for the TROR reporting. The amounts included with theTROR are required to reconcile to the DoD agency's audited financial statements. Furthermore,the certification of the TROR indicates that the delinquent debt amounts reported on the Receivables Report for cross-servicing and Treasury offset are correct and legally enforceable.

Due to the results of control deficiencies issued in the FY 2020 financial statement audit, DISA took action in documenting an internal control environment and various control activities for ARprocesses. DISA relies on its service organization to complete, compile, and certify the TROR and MRD Reports for DISA's WCF. DISA's service organization reviews DISA's inputs in FAMIS-WCF and populates the standard template package with the public AR data. DISA's service organization's personnel reconcile the MRD Report to the trial balance (TB) and submitsthe final TROR package to DISA for review, prior to its transmission to Treasury. The new process implemented due to its corrective action plans (CAP) involves DISA performing a review and tying out the TROR, noting DISA management's Common Access Card (CAC) signature, and DISA management is responsible for the oversight of the review of its service organization's documentation created on behalf of DISA.

Condition: DISA did not have its TROR and MRD Report review, approval, and reconciliationcontrols in place for the entire FY. As of Q2 of FY 2021, DISA had not yet implemented the new control to review and approve the TROR, prior to its service organization submitting the package to Treasury on behalf of DISA. DISA did not perform its review over the TROR and MRD Report package and reconciliation until April 2021; thus, there was not yet proper oversight and review of the TROR and MRD data from DISA's service organization.

Cause: DISA did not fully implement its new processes and controls related to AR for the entireFY under audit. As of Q2, DISA had not yet performed testing nor formally implemented the new processes and controls in response to the FY 2020 finding in order to validate the review over the accuracy of the support created by DISA's service organization on behalf of DISA.

Additionally, DISA's internal control program does not yet include a risk assessment that links risks to financial statement lines or assertions. It also does not include testing controls to ensure they address the applicable financial reporting objectives; updates to the internal control programwill help to identify and remediate control gaps.

Effect: Without an effective review of the data from FAMIS-WCF and the MRD Report data, aswell as the appropriate DISA management oversight controls in effect, DISA WCF may not be able to account for variances noted within the TROR and MRD Report submissions and record

complete AR balances. There is an increased risk that, without DISA management oversight of its service organization, the TROR and Public AR balance may result in a potential misstatementon the DISA WCF financial statements.

Recommendations: Kearney recommends that DISA continue to properly document and implement the procedures created within the FY 2021 financial statement audit and coordinatewith its service organization to perform the following:

1. Ensure that the AR control environment incorporates any updates to the monitoring controls and review of DISA's AR balances and its service organization reconciliations.
2. Continue to reconcile, monitor, and review the TROR and MRD Report compiled by its service organization and provide DISA management's approval of the data inputs prior to the service organization's submission to Treasury on behalf of DISA.
3. Perform a review and comparison over the MRD Report and TROR data variances and document its review throughout the process.
4. Continue to analyze, monitor, and test the performance of the reconciliation between the MRD Report and TB data to determine the need for any potential adjustments.
5. Update and continue to document any changes made to the MRD Report and TB reconciliation within the SOP.

3. Untimely Implementation of Controls for Allowance for Doubtful AccountsEstimate by Defense Information Systems Agency Management

Background: DISA relies on its service organization to create the applicable journal entry (JE),as well as create and obtain the necessary support for the Allowance for Doubtful Accounts estimate completed on a quarterly basis. An allowance for estimated uncollectible accounts should be recognized when it is more likely than not that the receivables will not be totally collected. These allowances should also be re-estimated on each annual financial reporting date,as well as when information has been obtained that the latest estimate may not be correct. The estimates are created from the receivables that arise from claims to cash or other assets against another entity, which have not yet been received or paid. An allowance for doubtful accounts should be recognized to reduce the gross amount of receivables to its net realizable value.

DISA documented a new control relating to the review of its service organization's Allowance for Doubtful Accounts JE package, which includes documenting DISA management's approval of the workbook and documentation support to confirm the accuracy of the JE package. DISA management is responsible for reviewing the estimates created by its service organization, whichare developed based on assumptions and relevant factors, prior to the posting of the transactions within the financial accounting system.

Condition: As of Q2, DISA implemented a new control to review and approve the Allowance for Doubtful Accounts JE package completed by its service organization. In Q2, DISA began itsmanagement oversight review for the work that its service organization completes on behalf of DISA's. Prior to Q2, DISA did not document a consistent review of the package and calculations created for the Allowance for Doubtful Accounts balance, which were completed by

its service organization prior to its inclusion in the financial statements. DISA had not outlinedconsistent formal controls or documentation in place to ensure there was DISA management review of the support obtained by its service organization to create the estimate amount.

Cause: DISA did not fully implement its new processes and controls related to AR for the entire FY under audit. As of Q2, DISA had not yet performed a test for reasonableness of the estimation and assumptions utilized by its service organization prior to that quarter and formally implemented its approval controls of the DISA oversight review. Additionally, DISA's internal control program does not yet include a risk assessment that links risks to financial statement linesor assertions. It also does not include testing controls to ensure they address the applicable financial reporting objectives; updates to the internal control program will help to identify and remediate control gaps.

Effect: Without appropriate documented review and approval of significant accounting balancesand estimates, such as the Allowance for Doubtful Accounts, DISA's WCF may not account forvariances in a timely manner, resulting in potential misstatements in the DISA WCF financial statements.

Recommendations: Kearney recommends that DISA continue to execute the CAPs in place for the FY 2021 financial statement audit and coordinate with its service organization to perform thefollowing:

1. Ensure that the AR control environment incorporates any updates to the monitoring controls and review of DISA's AR balances, as well as its service organization's creation of the estimates and JV.
2. Perform testing and review of the document internal controls to ensure the accuracy of the Allowance for Doubtful Accounts estimate.
3. Communicate and monitor the calculations and data created by its service organization and provide necessary feedback and timely approval to confirm the necessary estimate over the outstanding AR balances.
4. Continue to update and review the SOP and narratives to accurately reflect the input and management review.

B. Unmatched Transactions and Lack of Collection Validations

1. Unmatched Disbursements and Collections

Background: DISA WCF is composed of two divisions: Telecommunications Services and Enterprise Acquisition Services (TSEAS) and Computing Services (CS). DISA participates in Reimbursable Work Order – Grantor (RWO-G) transactions with its intragovernmental trading partners. Within an RWO-G agreement, DISA grants reimbursable authority to another Federal entity that performs the work stipulated in the agreement and bills DISA in order to replenish thefunding that it expended on DISA's behalf. In this process, DISA, through its service organization, reimburses its trading partners using IPAC or the 1080 collection process. DISA is responsible for ensuring goods/services were received and billings were accurate, consistent withthe RWO-G.

Condition: DISA and its trading partners initiate payments and collections through DISA's service organization without prior approval or authorization from its respective trading partner. DISA's current business process and control structure is set up to allow intergovernmental payments and collections to record in FAMIS as "unmatched" when a valid obligating documentand associated Accounts Payable (AP) or AR is not established beforehand. When an unmatched transaction occurs, DISA is required to perform an extensive manual effort after the unmatched payment or collection is recorded in FAMIS in order to ensure the payment or collection made by DISA's service organization belongs to DISA and appropriately matches to an obligation, payable, or receivable in FAMIS. In some cases, the processing of unmatched transactions can result in misstatements to multiple financial accounts.

As of September 30, 2021, the following amounts remained unmatched:

- $1.6 million disbursements
- $146 thousand collections.

Cause: DISA has engaged a service organization to process collections and disbursements that pertain to expenses and revenues on the agency's behalf. During FY 2021, DISA implemented aprocess to request, review, and post the appropriate accounting entries in FAMIS before disbursements are made, which significantly reduced the unmatched balances reported on September 30, 2021. However, unmatched disbursements and collections can still occur becauseDISA's service organization processes transactions, regardless of whether DISA has recorded a valid obligation/order or AP/AR transaction in advance of the activity.

Effect: Unmatched transactions that remain unresolved for the period ended September 30, 2021could potentially cause misstatements to the AP, AR, (Balance Sheet), and Gross Costs/ Revenues (Statement of Net Cost) financial statement line items. Unmatched disbursements andcollections create the risk that DISA's funds can be assigned erroneously by other Federal entities, DISA may be paying for goods and services that were never received, and DISA could potentially be paying inaccurate amounts. In some cases, after completing the manual research to clear an unmatched transaction, DISA must record adjustments to correct the misstatements initially caused by the unmatched transaction.

Recommendations: Kearney recommends that DISA perform the following:

1. Continue to coordinate with its service organization to ensure payments and collections made on behalf of DISA have an obligation or order and associated AP or AR transaction in FAMIS to liquidate against.
2. Implement controls and coordinate with its service organization's personnel to confirm the accuracy and existence of expense and revenue transactions prior to the payment and collection delivery to DISA's customer agencies. This could include DISA's service

organization providing DISA the invoice associated with payment to post in FAMISbefore the payment is processed.

3. Continue to research and resolve unmatched transactions timely, including the manual correction of misstatements caused by the transactions.

2. Lack of Monitoring and Assigned Criteria of the Defense Information SystemsAgency's Manual Collections Transactions

Background: Receivables arise from claims to cash or other assets against another entity. DISA's business process consists of its service organization processing collections received fromDoD and Non-DoD entities on behalf of DISA. DISA's collections are received via automated or manual methods. DISA's service organization receives manual collections through the SF- 1080 Print (PRN) process in the following classification categories: FedWire, Automated Clearing House (ACH)/Credit Card (Pay.Gov), and Physical Checks. The manual collections processed for the FedWire/ACH/Physical Checks transactions primarily occurs at DISA's service organization, and each transaction received flows through the service organization prior to any involvement of DISA personnel. DISA's service organization manually records the transactions that flow through FedWire and ACH on a spreadsheet as the transactions are received at DISA's service organization on behalf of various agencies. Specific to DISA WCF, the transactions noted within the SF-1080 PRN process account for approximately $8.2 million as of April 30, 2021. DISA's service organization is responsible for collecting these payments from the entities and ensuring that the collections are credited to DISA. However, DISA is responsible for monitoring its service organization to ensure that the applicable collections are recorded and apply to DISA.

DISA relies on its service organization to track the receipt of manual collections and determine which payments pertain to DISA. The collections received via the FedWire, ACH, and Physical Checks processes may not arrive with any specific data to identify and link it to an agency, and each transfer from the service organization relies on the personnel to determine the applicable receiving agency. Additionally, the Collections Team at DISA's service organization relies on their individual knowledge and prior experience in determining the applicable entity to assign thecollection amount. DISA's service organization noted that there were processes in development to assign account numbers to Commands, which will then allow the service organization to automatically transfer the FedWire transaction to the applicable agency.

In January of FY 2021, DISA implemented new processes to reach out to the Mission Partners (MP) using the 1080-PRN billing method to reconfirm their use of the 1080-PRN as their method of payment. As of January 27, 2021, DISA reached out to all associated MPs and customer agencies confirmed which methodology of payment was associated with their collection process. Additionally, DISA also implemented a new process to sample FedWire/ACH and Physical Checks to review the accuracy of the payment recording on a quarterly basis. However, DISA will need to rely on DISA's service organization's remediationefforts to complete its updates to the collections process, monitor the transactions, and confirm the applicable agencies.

Condition: DISA and its service organization had not fully implemented a process to maintain the appropriate criteria and assigned account number to support manual collections received and their applicable agency/customer, which would result in unmatched collections. As of Q3, DISAhad not finalized the internal control procedure for the implementation of its monitoring of its service organization to confirm and reconcile that the collections received via the FedWire/ACH/Physical Check processes are credited to the proper DISA account or the corresponding bill, resulting in potential unmatched collections.

Cause: DISA has not provided oversight over the collections process in place at its service organization to ensure that the collections received through the various methods of collection have a proper review or agency-specific reconciliation prior to the acceptance and processing byits service organization on behalf of DISA. DISA has not implemented effective controls to monitor and review the listing of customer agencies in place at DISA's service organization to ensure the applicable agencies are being credited for collections received and processed by DISA's service organization on behalf of DISA and other DoD entities.

Effect: Without appropriate monitoring and a formalized, official customer listing in place at DISA's service organization, there is an increased risk that DISA could receive FedWire/ ACH/Physical Check transaction collections that may not be related to DISA's operations or transactions and, thus, are credited to the incorrect customer. Additionally, DISA, in coordination with its service organization, determines the applicable agency, coordinates withthe MPs/Agencies, and applies the necessary research for any incoming collections that may remain unmatched to a DISA billing document.

Recommendations: Kearney recommends that DISA coordinate with its service organization toperform the following:

1. Design, coordinate, and implement a process to document and perform a quarterly review of a formalized listing of DISA's customer agencies to ensure the listing continues to be updated and revised for any incoming FedWire/ACH/Physical Check collections received at DISA's service organization on behalf of DISA to account for the accurate recording of the receivables.
2. Coordinate with its service organization to continue to implement and establish the current process to assign account numbers to Commands to automatically apply the applicable agency that is associated with the received wires.
3. Increase the review and communication of the agencies submitting collections, as well as continue to monitor the process completed at DISA's service organization on behalf of DISA to ensure there is an appropriate understanding between DISA and its service organization on the responsibilities, as well as update necessary documentation noted within the SOP.

C. Lack of Accounts Payable/Expense Accrual Validation

Background: A liability is a responsibility of a Federal Government agency to provide assets orservices to another entity at a determinable date, when a specific event occurs, or on demand.

Federal agencies should only record a liability when there is a probable and measurable future outflow or other sacrifice of resources as a result of past transactions. The United States Standard General Ledger (USSGL) provides guidance on which USSGL accounts should be usedto report the various types of liabilities that a Federal entity may encounter.

When a Federal agency is preparing financial statements, a methodology for estimating amounts owed, but not yet invoiced, must be established. This AP estimate ensures expenses are recordedin the proper period using accrual accounting and the matching principle. Management is responsible for developing these reasonable estimates based on assumptions and relevant factors and comparing estimates with subsequent results to assess the accuracy of the estimation process.

When there is a lag between the receipt of the good or service and the vendor invoice, expenses must be accrued to recognize the costs in the actual period the goods or services were received inaccordance with GAAP. An AP accrual is intended to recognize amounts owed by DISA for goods and services received, but not yet invoiced, and amounts invoiced, but not yet paid at the end of the accounting period.

Condition: DISA WCF records estimated expenses based on the burn rate of each individual type of contract (i.e., Firm Fixed Price [FFP], Cost-Plus Fixed Fee [CPFF]) estimation methodologies ranging between 80-99% of the total contract value over the period of performance specified in the signed contract agreements. This estimate is based on historical contract execution data. DISA determined this estimate by reviewing its history of completed contracts and the expenses incurred compared to contractual ceiling values. DISA has not successfully implemented a process or control to analyze subsequent vendor invoices paid to determine which FY the underlying goods and services were received. Such an analysis wouldprovide a validation of whether the estimated AP reported at period end was accurate.

Cause: DISA has not developed or successfully executed a process to validate its AP accrual estimates through a review of documentation that supports when the goods or services were actually received. In FYs 2020 and 2021, DISA initiated a process to attempt to perform this validation. DISA's validation process only recalculated the estimated AP balance in the prior period. This methodology was ineffective because DISA did not use the actual invoices from thesubsequent period to compare to and validate the accuracy of the estimated AP balance as of September 30. During FY 2021, DISA began the process of reperforming the lookback analysis to incorporate Kearney's recommendations below.

Effect: Without a process to validate the reasonableness of significant accounting estimates, the estimates may be based on assumptions that are not consistent with actual events and data. This increases the risk that DISA's financial statements may be misstated. Additionally, performing the analysis on the accrual population instead of the subsequent expense or disbursement population increases the risk that subsequent disbursements that should have been accrued are not being properly accounted for.

Recommendations: Kearney recommends that DISA management perform the following:

1. Continue to execute its plan to perform an accrual validation through the review of subsequent vendor invoices. DISA should compare actual vendor invoice amounts to the estimated AP balance to assess the reasonableness of the estimate.
2. Reassess the reasonableness of the AP estimation technique and its underlying assumptions based on the results and conclusion of the validation effort.

D. Lack of Receipt and Acceptance

1. Lack of Intragovernmental Payment and Collection System Receipt and Acceptance Process

Background: DISA participates in RWO-G transactions with its intragovernmental trading partners. Within an RWO-G agreement, DISA grants reimbursable authority to another Federal entity that performs the work stipulated in the agreement and bills DISA in order to replenish thefunding that it expended on DISA's behalf. In this process, DISA, through its service organization, reimburses its trading partners using IPAC.

The IPAC system allows intragovernmental entities to transfer funding between one another as reimbursement for goods and services provided. This system is configured to allow the service organization to process payments without prior approval from the receiver of those goods or services. These disbursements and collections are reported to Treasury on a monthly basis by itsservice organization, and DISA allows its service organization to accept and create payments on its behalf. DISA retains responsibility for ensuring it has sufficient appropriate documentation tosupport the payment.

Condition: DISA does not consistently obtain, review, or document the receipt and acceptanceof goods and services received from intragovernmental trading partners prior to payment.

Cause: DISA has engaged a service organization to process disbursements that pertain to expenses on the agency's behalf. DISA has not developed or implemented a formalized process with supporting internal controls to validate trading partner activity prior to payment via evidence of receipt and acceptance. DISA has not developed or implemented a process to obtainpost-payment evidence of receipt.

Effect: Without appropriate receipt and acceptance of trading partner activity, DISA is not able to confirm the accuracy, validity, or timeliness of its intergovernmental transactions (both Gross Costs and AP). As a result, DISA may have misstatements in its Gross Costs and AP in the period it receives goods and services, as well as additional misstatements in the subsequent period when the Gross Costs and AP are recorded. DISA is at increased risk of paying trading partners for goods or services that did not conform with the terms of its agreements or that DISAnot receive.

Recommendations: Kearney recommends that DISA coordinate with its service organization toperform the following:

1. Design, track, and implement G-Invoicing and ensure the process is mitigating the issues identified in the condition accordingly.
2. Design and implement a process to validate and document receipt and acceptance of goods/services provided by intragovernmental trading partners.
3. Coordinate with trading partners to ensure Support Agreements (SA), Inter-Agency Agreements (IAA), Memorandums of Understanding (MOU), or equivalent include language requiring cooperation of the trading partner to provide any required documentation necessary for DISA to validate the accuracy of the amounts that have been billed.
4. Implement controls and coordinate with its service organization's personnel to confirm the valuation and existence of expense transactions prior to the payment delivery to DISA's customer agencies.

2. Lack of Documentation Reflecting Wide Area Workflow Receipt and Acceptance

Background: DISA WCF procures various telecommunication and computing goods and services throughout the year with both DoD and Non-DoD agencies. DISA receives invoices forthe procured goods/services through the Wide Area Workflow (WAWF) system. A majority of these transactions are invoiced through the system. WAWF provides the DoD and their suppliers with a single point of entry to generate, process, and store invoices, receiving reports, non-contractual payment requests, and acceptance data sets, as well as other related data to support DoD asset visibility, tracking, and payment processes by a systematic flow for agencies. It provides the connection of information related to the acceptance of goods and services in support of the DoD supply chain. WAWF has a System and Organization Controls (SOC) 1® report that is completed each FY in order to assess the specific systematic controls, as well as to identify the complementary user entity controls (CUEC) that the user entity (i.e., DISA) has the responsibility to implement to support WAWF transactions. As described in ***Exhibit 2*** and Section I.F, *Incomplete Complementary User Entity Controls Implementation*, DISA has not implemented all of the CUECs required by its service organizations.

WAWF system end users include vendor technicians entering the invoice detail, as well as the specific Contracting Officer's Representatives (COR) who approve orders within WAWF, whichinitiates payment. WAWF's program office encourages the user entities to implement the entity's own policies and procedures relating to what is required to be confirmed for each WAWF transaction. The WAWF process is initiated by the vendor, who is providing goods/services to DISA, loading the invoice detail (e.g., amounts, Contract Line Item Number [CLIN], description of goods and services, date received) into WAWF. The vendor submits this summary of the invoice information and can also upload an electronic copy of the invoice from the vendor's accounting system for additional support as an attachment within WAWF. The COR is responsible for verifying the vendor attachments in WAWF, ensuring the transaction is accurate and valid, as well as uploading evidence of receipt into WAWF.

Condition: DISA does not have a process in place to consistently validate the supporting documentation submitted by vendors and approved by the COR prior to certification and payment. DISA has not implemented a consistent process to document evidence of the review ofthe invoice, receiving report, and contract/purchase request. Additionally, DISA has not implemented the CUECs from the WAWF SOC 1® report regarding obtaining and maintaining sufficient support to document evidence of receipt and acceptance of goods and/or services.

Cause: DISA management places reliance on the general functionality of the WAWF environment in order to perform a systematic receipt and acceptance of the transactions. The COR within DISA and its customers do not have a consistent methodology to retain the supporting documentation of their concurrence, in having received the specific goods/services asnoted by their systematic approval. DISA has chosen not to outline or document a policy in place to emphasize the COR's retention of supporting documentation per the WAWF SOC 1® report, which is documented as a key responsibility of DISA. DISA has not developed an effective remediation approach, as it relates to the WAWF SOC 1® report, which would provideincreased controls outside of the WAWF system and collaboration between the system and the user entity (DISA).

Effect: Without appropriate review of the supporting documentation submitted and attached forreceipt and acceptance within WAWF, there is an increased risk that DISA has not received thegoods or services described in the vendor invoice. CORs who are responsible for receipt and acceptance will have varying decisions on what documentation would prove acceptance, thus resulting in inconsistency across DISA. DISA is not able to support the accuracy, validity, or timeliness of its receipt and acceptance in instances where the invoices are not submitted with applicable descriptions of the goods or services, whether that is on a timely basis or billed erroneously. Ineffective controls or control objectives may result from DISA's failure to implement internal controls to address all required CUECs.

Recommendations: Kearney recommends that DISA management perform the following:

1. Design and implement a standardized process to perform a three-way match between the invoice, receiving report, and contract/purchase request in order to validate the documentation of the receipt and acceptance of goods and/or services provided by vendors through WAWF.
2. Design and implement the CUEC described in the WAWF SOC 1® report to ensure that the COR consistently reviews and documents evidence of the receipt and acceptance of the goods and service prior to approving the invoice in WAWF. This may include updating the SOP and COR training to meet those requirements.

3. Lack of Implementation of Review and Revalidation Tool over TelecommunicationsServices and Enterprise Acquisition Services Pass-Through Telecommunication Transactions

Background: A significant portion of TSEAS revenue is "pass-through" revenue. Pass-throughrevenue occurs when a customer contacts TSEAS to procure or provide a specific good or service.

After the customer contacts TSEAS requesting goods or services, DISA contracts with an outsidevendor to provide the goods or services. DISA incurs expense to the outside vendor and revenueto the requesting agency (customer). Per the individual contracts between DISA and the requesting agency, the customer is responsible for notifying DISA WCF TSEAS if there is a change or update needed for the provided service. DISA has been in the development stages of anew reporting tool that allows DISA WCF customers to monitor its services for review and revalidation. Once this tool is implemented, DISA will have the ability to obtain enhanced documentary audit evidence, through review and revalidation of existing services, that revenue isrecognized for actual services delivered and expenses are approved for actual services received.

Condition: DISA WCF acts as the intermediary agency to procure telecom services for the requesting agency by facilitating a "pass-through" contractual service. Many of these agreements include monthly recurring charges (MRC), which automatically generate expense and revenue each month over the life of the contract. DISA's customer, the requesting agency, isresponsible for notifying DISA WCF if there was a disruption in service or a need to update or cancel a recurring service. DISA has not yet implemented a review and revalidation tool, which will provide assurance to DISA WCF that its customers' services were received and active throughout the life of the contract.

Cause: DISA was still in the process of implementing the tool to serve as a control relating to the communication, review, and revalidation of whether the requested services were still active or if there was a need for an updated/cancelled service. Accordingly, DISA has not yet updatedits internal control documentation related to this process. DISA anticipates that the controls andrelated processes will be in place during FY 2021 or early FY 2022.

Effect: Without proper documentation, testing, and monitoring of the review and revalidation tool, pass-through activity could result in invalid or unnecessary usage of services. As there is no control in place, DISA WCF is not able to review the "pass-through" activity tool customer responses to determine if service is still active and required. DISA lacks the necessary controlsto assert valid receipt and acceptance over telecommunication pass-through transactions.

Recommendations: Kearney recommends that DISA communicate with its "pass-through"customer agencies and perform the following:

1. Establish and implement policies and procedures to review the tool used to review and revalidate the telecommunication agreements throughout the FY.

2. Coordinate with requesting agencies to implement the use of the review and revalidation tool appropriately so DISA WCF can ensure there is a present need for the provided services.
3. Update the SOP and the necessary training for DISA personnel to determine the actions needed for each telecommunication "pass-through" transaction.

E. Lack of Operating Effectiveness Relating to the Certification and Documentation ofTravel Expense

Background: DISA personnel travel for various reasons to other DISA locations or Government agencies. Travelers utilize the Defense Travel System (DTS), which is a fully integrated, electronic, end-to-end travel management system that automates temporary duty (TDY) travel approvals and transactions for the DoD. DTS allows travelers to create authorizations, book reservations, receive necessary systematic approvals, generate vouchers for reimbursement, and direct payments to the travelers' bank accounts. When DISA personnel are directed to travel, thefirst-line approver will initially approve the travel via an e-mail correspondence between the traveler and supervisor.

In order to become an authorized Travel Certifying Officer (CO), the appointee must complete the necessary trainings and requirements, as well as sign the Department of Defense (DD) 577, *Appointment/Termination Form*. Officials within the agency/organization with the appointing authority will approve and sign the DD 577. The CO/Approving Official (AO) will log into DTSto review and approve the traveler's submission package after the traveler documents and submits all of his/her applicable receipts within DTS.

DISA and its service organization are responsible for maintaining the applicable documentation to support the approval authority, as well as the travel expenses incurred throughout the FY. In response to its remediation efforts, DISA management developed a CAP, which highlighted the development and maintenance of a repository of DD 577s to better support the current CO/AO'sapproval of the DTS actions, but it had not fully executed those procedures in FY 2021. DISA continues to work internally on its DTS internal controls and is responsible for monitoring its service organization to provide the necessary support of the travel expense transactions specific to DISA.

Condition: DISA did not fully implement processes to maintain appropriate documentation andDTS controls to support expense transactions. DISA was unable to execute the following:

- Twenty-eight of 78 samples did not have valid DD Form 577 supporting documentation
- Forty-four of 78 samples did not have proper documented evidence of approval or timely approval of 36 of 78 DTS travel orders and 16 of 78 DTS travel vouchers
- Seventeen of 78 samples were not recorded in the proper period
- Thirty-six of 78 samples did not have documentation provided to support the transaction amount.

Cause: In FY 2021, DISA developed a CAP, but it had not fully executed the procedures to remediate the finding. Although DISA did create a repository for its DD 577s, the control did not yet result in the necessary documentation for all the appropriate approval designations of theAOs/COs. DISA also did not implement internal controls to monitor that the travel approvals were performed in a timely manner and all relevant AO approval stamps were documented within DTS. DISA did not perform testing or an appropriate review to determine that the applicable period and recording of the gross costs were performed in a timely manner and the expenses were posted in the proper period.

Effect: Without appropriate review of the travel expenses and the applicable DD 577s, there is an increased risk that DISA's travel expenses are misstated and that there could be transactionsthat do not have the appropriate approval authority. DISA is not able to adequately support a timely and appropriate review over the travel process. As a result, ineffective controls or a lackof control objectives may result in the travel approvals to be inaccurate.

Recommendations: Kearney recommends that DISA coordinate internally, as well as with itsservice organization, to perform the following:

1. Continue to implement and test the CAP remediation efforts in place to further develop the WCF travel control environment.
2. Further develop and monitor a consistent process for timely approvals of travel expenses and ensure the necessary supporting documentation for the various types of transactions are adequately maintained and clearly documented within DTS, as well as for audit requests.
3. Continue to retain and maintain the applicable DD 577s for DISA's CO/AO, as well as ensure that the process to become a CO or AO is completed timely with the proper approval documentation.
4. Ensure there is an appropriate understanding between DISA and its service organization relating to the responsibilities of processing travel transactions, retaining documentation to be readily available for request, and updating the necessary processes noted within the SOP.

III. Budgetary Resources *(Repeat Condition)*

Deficiencies in two related areas, in aggregate, define this material weakness:

A. Lack of Lookback Analysis over Dormant Control
B. Untimely Undelivered Order Transactions

A. Lack of Lookback Analysis over Dormant Control

Background: Undelivered Orders (UDO) represent the amount of goods and/or services orderedthat have not been actually or constructively received; these can be unpaid or prepaid. Federal agencies record UDOs when they enter into an agreement, such as a Military Interdepartmental

Purchase Request (MIPR), contract, or sales order, to receive goods and/or services. Agenciesshould maintain policies and procedures to ensure that UDOs represent valid future outlays.

Unfilled Customer Orders (UCO) Without Advance, USSGL Account 422100, represent orders for goods and/or services to be furnished for other Federal Government agencies and for the public. Federal agencies record UCOs Without Advance when they enter into an agreement, such as a MIPR, contract, or sales order, to provide goods and/or services when a customer cashadvance is not received. These orders provide obligational budgetary authority for reimbursableprograms. Agencies should maintain policies and procedures to ensure that UCOs represent valid future billings and collections.

The DISA WCF reported more than $2.9 billion in UDOs and $2.8 billion in UCOs on its September 30, 2021 TB. The UDO account balance is supported by a subsidiary ledger that details information, such as the document number, obligated amount, undelivered amount, andtransaction date, among other unique identifying details for each UDO balance. The UCO account balance is supported by several subsidiary ledgers that detail information, such as the customer, order number, order amount, and transaction date, among other unique identifying details for each UCO balance.

In remediation efforts, DISA developed a quarterly control to identify UDO balances that are unlikely to be delivered. The control was designed to record an accounting adjustment for UDOsthat remain open 18 months beyond the period of performance and were recorded to a Purchase Order (PO) that did not have any invoice activity on any of the contract line items or delivery orders within the last calendar year. The UDO adjustment was $350.6 million as of
September 30, 2021.

In response to prior-year Notices of Findings and Recommendations (NFR), DISA developed a quarterly control to identify UCO balances that are unlikely to be fulfilled. The control was designed to record an accounting adjustment of UCOs for Reimbursable Projects related that fund UDOs that remain open 18 months beyond the period of performance and were recorded toa project that did not have any invoice activity that are in a high-risk category of not being delivered. The control was designed to record an accounting adjustment for UCOs that fund UDOs that remain open 18 months beyond the period of performance and were recorded to a project that did not have any invoice activity or delivery orders within the last calendar year.
The UCO adjustment was $267.6 million as of September 30, 2021.

Condition: DISA does not have documented controls in place to perform a lookback analysis over its process to adjust its budgetary accounts for dormant balances. While DISA has established controls to write down dormant UDOs and UCOs Without Advance, DISA does nothave a documented control to perform a lookback analysis to determine how many accounts determined to be dormant later received invoices. This documented lookback analysis will helpensure that the criteria determined in the dormant balance control is based on the most appropriate assumptions.

Cause: Although DISA developed a control to adjust account balances for UDOs and UCOs thatare unlikely to be delivered, it did not perform a lookback analysis over the control to ensure the underlying assumptions for the controls were still appropriate. Had DISA performed a robust risk assessment covering all assertions related to the New Obligations and Upward Adjustments and Spending Authority from Offsetting Collections line items on the Statement of Budgetary Resources (SBR), they may have better identified the risks of misstatement and identified the need to perform a lookback analysis over the dormant UDO and UCO control.

In previous years, DISA management indicated that dormant balances remain open and reportedin the financial statements due to the lack of effective reviews for validity by funds holders, delays in contract close-out processing by DISA's Procurement Services Directorate (PSD), delays in Defense Contract Audit Agency (DCAA) audits, and the need to reconcile and de- obligate aged funding balances during the life of the contract. DISA officials indicated that theywere reluctant to de-obligate individual amounts in the detailed accounting records until these steps have been completed.

Effect: Failure to design and document controls over the lookback analysis of the dormant obligations increases the risk that DISA may adjust its budgetary accounts on insufficient assumptions. Additionally, DISA may misstate the New Obligations and Upward Adjustmentsline and Spending Authority from Offsetting Collections line on the FY 2021 SBR.

Recommendations: Kearney recommends that DISA perform the following:

1. Implement and document a lookback analysis over the dormant controls to ensure the controls to adjust its budgetary accounts are based on the most appropriate assumptions.
2. Update existing policies to ensure that funds holders are adequately assessing the validity of the open UDO balances and de-obligate invalid UDOs, when possible.
3. Implement policies, or update existing policies, to require PSD to process contract actions timely once all goods and services have been provided to the customer.
4. Update its internal control program so that the risk assessment is linked to financial statement assertions.

B. Untimely Undelivered Order Transactions

Background: An obligation is a legally binding agreement that will result in outlays, immediately or in the future. When an agency places an order, signs a contract, awards a grant, purchases a service, or takes other actions that require the Government to make payments to the public or from one Government account to another, it incurs an obligation. Agencies should maintain policies, procedures, and information systems to ensure that obligations represent required Federal outlays, comply with laws and regulations, and are appropriately approved. TheDISA WCF reported approximately $2.9 billion in UDO on its September 30, 2021 TB.

Starting in FY 2021, DISA recorded a JV when an obligation was not able to be recorded in FAMIS within 10 days. DISA reversed the JV once the obligation was entered into FAMIS, and

the JVs are tracked on a JV log. DISA is responsible for establishing controls to ensure UDOsare entered into the financial management system timely.

Condition: As of Q3, DISA recorded 19 obligations, totaling $125.5 million, out of 327 sampled obligations that were not entered into the financial management system or recorded by JVs within 10 days of the execution of the obligating document.

Cause: DISA did not have effective transaction-level control procedures to ensure obligations were recorded in the financial management system in a timely manner in accordance with DoD Financial Management Regulation (FMR), Volume 3, Chapter 8, Section 080303. Further, DISA did not have effective agency-wide monitoring controls to ensure timely recording of contracting actions. DISA's internal control program does not yet include a risk assessment thatlinks risks to financial statement lines or assertions. It also does not include testing controls to ensure they address the applicable financial reporting objectives. Such risk assessment and test procedures may have enabled DISA to identify the necessary control activities related to recording obligations timely. Updates and improvements to the internal control program will help to identify and remediate control gaps.

Effect: Obligations that are not recorded in a timely manner increase the risk that:

- Goods or services may be acquired and/or received prior to an authorized obligation certifying the availability of funds or prior to an authorized contract or purchase order being established. The process of authorizing the obligation and certifying funds availability ensures the completeness of the recorded obligation balances
- The Antideficiency Act could be violated. If obligations are not recorded prior to the acquisition of goods and/or services, the agency could obligate more funds than it was appropriated
- Payments may not be made in a timely manner in compliance with the Prompt Payment Act of 1982.

Recommendations: Kearney recommends that DISA perform the following:

5. Update controls to ensure the timely creation, approval, and recording of obligations. Specifically, DISA should implement controls at the obligation level to ensure that obligations are recorded in a timely manner to support funds control.
6. Update its internal control program so that:
   a. The risk assessment is linked to financial statement lines and assertions.
   b. The control testing is designed to address the risks identified in the risk assessment and financial reporting objectives.

* * * * *

Significant Deficiencies

Throughout the course of our audit work at DISA, we identified internal control deficiencies which were considered for the purposes of reporting on internal control over financial reporting.The significant deficiencies presented in this Schedule of Findings have been formulated based on our determination of how individual control deficiencies, in aggregate, affect internal controlover financial reporting. ***Exhibit 2*** presents the significant deficiencies identified during our audit.

Exhibit 2: Significant Deficiencies

Significant Deficiency	Significant Deficiency Sub-Category
I. Financial Reporting	A. Lack of Documentation and Approval of Defense Information Systems Agency Management's Assessments Related to its Reporting Entity and Applicability of Insurance Programs per Statement of Federal Financial Accounting Standards Requirements B. Fourth Quarter Agency Financial Report Errors and Compliance
II. Information Technology	A. Financial Accounting and Budget System Application Audit Logging and Monitoring B. Incomplete Financial Accounting and Budget System Plan of Action and Milestones C. Incomplete Financial Accounting and Budget System Application Access Request Documentation D. Financial Accounting and Budget System Removal of Inactive and Separated Users E. Financial Accounting and Budget System Application User Periodic Access Review F. Incomplete Complementary User Entity Controls Implementation

I. Financial Reporting *(Repeat Condition)*

Deficiencies in two related areas, in aggregate, define this significant deficiency:

A. Lack of Documentation and Approval of Defense Information Systems Agency Management's Assessments Related to its Reporting Entity and Applicability of Insurance Programs per Statement of Federal Financial Accounting Standards Requirements
B. Fourth Quarter Agency Financial Report Errors and Compliance

A. Lack of Documentation and Approval of Defense Information System Agency Management's Assessments Related to its Reporting Entity and Applicability ofInsurance Programs per Statement of Federal Financial Accounting Standards Requirements

Background: FASAB's Statement of Federal Financial Accounting Standards (SFFAS) No. 47, *Reporting Entity*, was established to guide preparers of general-purpose Federal financial reports (GPFFR) in determining what organizations to report upon, identifying "consolidation entities" and "disclosure entities," determining what information should be presented for each type of entity, and identifying related parties. Additionally, SFFAS No. 51, *Insurance Programs*, established disclosure requirements for insurance programs in connection with a reporting entity's GPFFR. Agencies are required to disclose their applicability and document whether theyidentify any of the following: "1) exchange transaction insurance programs other than life insurance, 2) nonexchange transaction insurance programs, and 3) life insurance programs." DISA management is responsible for determining the applicable implementation and documenting their review over the FASAB standards and the SFFAS assessments within a timely manner to ensure auditability and proper application of the standards.

Condition: In its remediation efforts, DISA implemented a procedure to review the SFFAS guidance related to No. 47 and document any updates via a draft checklist and assessment. However, DISA did not complete a timely and documented assessment listing of DISA's Reporting Limits and Basic Symbols in order to define its financial reporting entity, which would ensure completeness of its financial statements and related disclosures in accordance withSFFAS No. 47. DISA had not completed or documented an assessment over SFFAS No. 51 to determine whether it has any applicable insurance programs for which disclosure is required.

Cause: Despite some efforts in FY 2021 to address prior-year recommendations, DISA has not analyzed, developed, or implemented sufficient controls to ensure that it has complied with and documented DISA's applicability with the requirements of SFFAS No. 47 to periodically confirm it has appropriately defined the various Components comprised in its reporting entity, inclusion of its Basic Symbols and Limits, and within a separately documented management- approved assessment, aside from the year-end footnote disclosures. DISA also has not implemented sufficient controls to ensure that it has disclosed and separately documented management's assessment, including the necessary information of its applicability of InsurancePrograms under the requirements of SFFAS No. 51.

Effect: There is an increased risk that the DISA financial statements may be incomplete as a result of the omission of consolidation entities and/or disclosure entities for which DISA's reporting entity may be accountable. Further, the Government-wide GPFFR may be incompleteas a result of any missing consolidation or disclosure entities for which DISA has not identified for its GPFFR. There also is an increased risk that the DISA financial statements do not includethe required disclosures for the applicability of insurance programs.

Recommendations: Kearney recommends that DISA perform the following:

1. Complete the analysis, development, and implementation of the controls and procedures to annually assess and re-validate its GPFFR financial reporting entity for completeness, as well as its applicability to the disclosure of insurance programs, in accordance with the provisions of SFFAS No. 47 and No. 51, respectively. The assessments should be formalized with appropriate review and approval from DISA management. The approved DISA reporting entity definition should be communicated to applicable stakeholders within the Office Under the Secretary of Defense (Comptroller) (OUSD[C]) and its service organization.
2. Maintain documentation to demonstrate the completion of the assessments, including the analysis performed, sources referenced, and conclusions reached. DISA should document the assessment process in the form of an SOP to ensure this process is consistently performed at the entity's policy level and performed by each reporting entity (e.g., WCF and General Fund [GF]).
3. Implement the controls and documentation mentioned in Recommendations #1 and #2 to ensure that the management assessments of SFFAS and its conclusions are properly reflected in DISA's respective footnotes.

B. Fourth Quarter Agency Financial Report Errors and Compliance

Background: DISA utilizes a service organization that is responsible for financial reporting. DISA's service organization performs financial statement compilation and reporting within the Defense Departmental Reporting System (DDRS) – Budgetary (B) and DDRS – Audited Financial Statements (AFS). DISA management is responsible for the compilation of financial information into DISA's Agency Financial Report (AFR), as well as the accuracy, completeness,and presentation and disclosure of the information reported within. DISA is also responsible for ensuring that the AFR is prepared and presented in compliance with OMB Circular A-136, *Financial Reporting Requirements*. Each quarter, including at FY-end, DISA management completes and signs a checklist of items and tasks to complete as it prepares its financial statements and financial statement notes and disclosures. In its remediation efforts, DISA's CAPindicated a final milestone date of June 30, 2021; however, based on review of the interim AFR and its contents, some remediation remains ongoing relating to CAP milestones that have not been achieved.

Condition: The DISA Q4 draft AFR contained errors, omissions, and inconsistencies not identified by DISA management. For example, errors were noted in Management's Discussionand Analysis (MD&A), the principal financial statements, and the notes and disclosures to the financial statements. DISA's draft AFR also omitted required components of the Other Information (OI) section, contained inconsistent information between different related parts of the AFR, and contained financial information that did not reconcile to underlying supporting documentation. The AFR also contained various editorial errors.

Cause: Although DISA has designed a CAP and implemented some process improvements during FY 2021, DISA does not yet have adequate review or quality control (QC) procedures toensure the content of the AFR is complete, accurate, and supported. DISA relies on its service organization to prepare its AFR with standardized DoD language throughout. The standard language populated by its service organization was not always adjusted by DISA management based on the specifics of their organization and financial position. DISA management's quarterly checklist for the preparation of its AFR did not ensure that the AFR was complete, accurate, and in compliance with OMB Circular A-136 requirements.

Effect: DISA made corrections and incorporation of the additional information to its FY 2021 AFR prior to finalization in order to ensure the document complied with the appropriate OMB requirements. However, without appropriate controls and QC processes, there is an increased risk that DISA's AFR will not be complete, accurate, and compliant with OMB requirements infuture periods.

Recommendations: Kearney recommends that DISA perform the following:

4. Continue to review, develop, implement, and document the processes and controls for the accumulation and review of data used to develop and prepare the AFR to ensure that disclosures, supporting tables, and analytical information reported in the AFR are accurate.
5. Continue to create, develop, and document additional procedures and/or checklists to:
   a. Identify all relationships of information within the AFR to ensure consistency in information presented.
   b. Ensure all the information compiled into the AFR is reviewed at a sufficient level by DISA management, in order to ensure accuracy, completeness, and compliance with requirements.
   c. Document evidence of the detail review(s).

II. Information Technology *(Repeat Condition)*

Deficiencies in six related areas, in aggregate, define this significant deficiency:

C. Financial Accounting and Budget System Application Audit Logging and Monitoring
D. Incomplete Financial Accounting and Budget System Plan of Action and Milestones
E. Incomplete Financial Accounting and Budget System Application Access Request Documentation
F. Financial Accounting and Budget System Removal of Inactive and Separated Users
G. Financial Accounting and Budget System Application User Periodic Access Review
H. Incomplete Complementary User Entity Controls Implementation

A. Financial Accounting and Budget System Application Audit Logging and Monitoring

Background: DISA personnel located at Fort George G. Meade (FGGM) and Scott Air ForceBase (AFB) are responsible for information system security management, including authenticator management for the Financial Accounting and Budget System (FABS). FABS manages and tracks the financial aspects (e.g., AP, vendor invoices, vouchers) associated withtelecommunication circuits, equipment, and services leased from various carriers/vendors on behalf of the Government through the WCF/TSEAS. FABS also supports customer billing, indicating MRCs, non-recurring charges, and overhead charges.

Monitoring activities or events within an application is a key control designed to detect suspicious behavior or malfunctions. For example, an organization should independently monitor modifications to existing users' accounts, such as changes to the permissions granted to an individual user. A common method to monitor application activities involves reviewing the audit log. An audit log is an automated record that contains specific events or activities within an application in an electronic form. For instance, a system or application administrator may set up the audit log to record instances when a new account is created, when security permissions foran existing account change, or to record unsuccessful login attempts by a user. The audit log enables administrators to have regular visibility into user access or other activities in a manageable way. When deciding which activities to capture in the audit log, an organization should consider its security requirements, the risk of loss, the volume of events the log will generate, and the utility of capturing the specific information. Once the audit log parameters are established, an organization should regularly investigate events or activities reported in the audit log or audit exception reports developed from the audit log.

Condition: DISA developed a process to log security authorization modifications (e.g., modifications to existing users' account privileges) for the FABS application; however, the process did not include review and documentation detailing how personnel would complete the review. For example, DISA did not document a process to perform a review, including the frequency of review, maintenance of review documentation, and documentation of actions takenas a result of the review.

Cause: In April 2021, DISA personnel implemented a process to log all security authorization modifications to the FABS application; however, due to timing constraints, DISA was unable to implement a review of the logs to include actions taken on account modifications captured, as well as documenting the process in DISA-specific policies and procedures.

Effect: By not reviewing and documenting the actions taken on the audit logs for the FABS application on a regular basis, DISA does not have reasonable assurance that it would identify inappropriate access or changes to application user accounts in a timely manner. In addition, failing to review audit logs for the FABS application increases the risk that a compromised administrator account may elevate an account's privileges, perform unauthorized activities, andreturn account privileges to the original state.

Recommendations: Kearney recommends that DISA perform the following:

1. Develop procedures to regularly review and document FABS security authorization modifications at the application layer. This documentation, at a minimum, should identify which events are logged, which events require manual review and why, who performs the review, the frequency of the review, how the individuals responsible for the review remain independent from reviewing their own work, how the logs are protected from inappropriate tampering, which events require escalation, and how the reviewers document and retain their review.
2. Implement the documented review process and retain evidence of the review of FABS application logs for third-party review.
3. Update applicable FABS policy and procedural documentation to reflect the newly developed application audit log and review process.

B. Incomplete Financial Accounting and Budget System Plan of Actions and Milestones

Background: DISA personnel located at FGGM and Scott AFB are responsible for informationsystem security management for FABS. FABS manages and tracks the financial aspects (e.g., AP, vendor invoices, vouchers) associated with telecommunication circuits, equipment, and services leased from various carriers/vendors on behalf of the Government through the WCF/TSEAS. FABS also supports customer billing, indicating MRCs, non-recurring charges, and overhead charges.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision (Rev.) 2, *Risk Management Framework for Information Systems and Organizations*, informs individuals associated with the design, development, implementation, operation, maintenance, and disposition of Federal information systems about how to conduct risk assessments, security categorizations, security control selections and implementations, securitycontrol assessments, information system authorizations, and monitoring of security controls.
Further, NIST SP 800-37, Rev. 2 requires that a designated AO authorize agency information systems to operate. As part of the authorization process, the agency must develop, track, and manage a comprehensive Plan of Action and Milestones (POA&M) for known system weaknesses. OMB Memorandum (M)-02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security POA&Ms*, provides specificPOA&M guidance to agencies, including guidance on sources of security weaknesses. DISA utilizes the Enterprise Mission Assurance Support Service (eMASS) to develop, track, and manage its POA&Ms.

Condition: DISA's POA&M management process did not capture all security weaknesses foundwithin the FABS application during reviews done by, for, or on behalf of the agency, as requiredby OMB Memorandum M-02-09. Specifically, DISA did not develop, track, and manage POA&Ms for security weaknesses found within FABS through NFRs issued during the FY 2020financial statement audit.

Cause: DISA management communicated the need to create a CAP for NFR #2020-IT-WCF-06, *Incomplete FABS Access Request Documentation*; however, they did not communicate the need to create POA&Ms for all FABS security weaknesses to personnel responsible for developing, tracking, and managing POA&Ms.

Effect: POA&Ms are a critical tool to help ensure that management tracks and resolves all weaknesses in a timely manner and presents the AO with all known weaknesses when making anauthorization decision. By not including all applicable security weaknesses in its formal POA&M process, DISA increases the risk that the AO may grant a system an authorization to operate without considering all relevant factors.

Recommendations: Kearney recommends that DISA perform the following:

4. Enhance its formal POA&M management process to ensure personnel responsible for developing, tracking, and managing POA&Ms are aware of all applicable security weaknesses per OMB Memorandum M-02-09, including those found during reviews done by, for, or on behalf of the agency (i.e., NFRs issued during financial statement audits).
5. Supplement its POA&M Tactics, Techniques, and Procedures (TTP) with an SOP, work instruction, or equivalent documentation to ensure a repeatable POA&M management process with consistent communication of security weaknesses from all required sources.

C. Incomplete Financial Accounting and Budget System Application Access RequestDocumentation

Background: DISA personnel located at FGGM and Defense Information Technology Contracting (DITCO) – Scott AFB are responsible for information system security management,including authenticator management for FABS. FABS manages and tracks the financial aspects(e.g., AP, vendor invoices, vouchers) associated with telecommunication circuits, equipment, and services leased from various carriers/vendors on behalf of the Government through the WCF/TSEAS. FABS also supports customer billing, indicating MRCs, non-recurring charges, and overhead charges.

DISA controls initial account access to the FABS application through the receipt of a completed and reviewed DD Form 2875, *System Authorization Access Request (SAAR)*, or a User Account Access Checklist depending on whether a user is external to the DITCO-Scott AFB location or internal. The SAAR for initial access to FABS requires the prospective user to complete securityawareness training, provide required personal information, and include the approval signatures ofthe user's supervisor and local security manager. In addition, the user indicates requested permissions within the form via Facility Code, which grants access to a specific set of application modules (e.g., FABS). The user's supervisor then submits an Information Technology Service Management (ITSM) ticket, assigned to the System Administrator (SA) group, to gather final approval by the data owner and processing. The SA group will identify theapplicable data owner, residing in DISA's Office of Accounting Operations and Compliance (CFA) or DITCO-Scott AFB Procurement Services Directorate (PL8). The data owner will

conduct the final review of the DD 2875 and indicate approval via signature or e-mail. Internalusers follow the same process as the external users; however, they complete a User Account Access Checklist in place of the SAAR.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, informs individuals responsible for information systems that approving and enforcing authorized access at the application provides increased information security.
Unapproved and inappropriate user access and privileges increases the risk to the confidentiality, integrity, and availability of the system and its data.

Condition: DISA was unable to provide sufficient documentation to support that managementreviewed and approved the access permissions for all three users granted access to the FABS application from October 1, 2020 through May 3, 2021. Specifically, DISA was unable to provide evidence of requested facility codes (e.g., permissions) or data owner approval for all three users.

Cause: In March 2021, DISA personnel updated the user authorization process for all DITCO systems, including FABS. These updates included procedures requiring formal approvals by users' supervisors and relevant data owners prior to creating user accounts, as well as maintaining completed access request documentation. However, DISA did not have an effectiveQC process to ensure personnel responsible for FABS user authorization followed the documented process.

Effect: By failing to ensure data owner approval prior to granting users access to the FABS application or documenting and validating requested roles, DISA increases the risk that usersmay receive inappropriate access to the FABS application.

Recommendation: Kearney recommends that DISA perform the following:

6. Develop and implement a QC review over the user authorization process. The QC process should include procedures to ensure completion of the SAAR and the User Account Access Checklist forms, validating requested roles and data owner approval. To gain efficiencies, DISA should consider incorporating this QC process as it conducts its audit log reviews of account creations and modifications.

D. Financial Accounting and Budget System Removal of Inactive and Separated Users

Background: DISA personnel located at FGGM and Scott AFB are responsible for informationsystem security management, including authenticator management for FABS. FABS manages and tracks the financial aspects (e.g., AP, vendor invoices, vouchers) associated with telecommunication circuits, equipment, and services leased from various carriers/vendors on behalf of the Government through the WCF/TSEAS. FABS also supports customer billing, indicating MRCs, non-recurring charges, and overhead charges.

DISA personnel control account access removal for the FABS application. The supervisors ofthe departed personnel, in conjunction with the System Administrators, are responsible for ensuring that access to the FABS application is terminated upon departure of the employee.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, informs individuals responsible for information systems that removing or disabling terminated or separated users access in a timely manner at the application provides increased information security. Inappropriate user access and privileges increase the risk to theconfidentiality, integrity, and availability of the systems and its data.

Condition: DISA personnel failed to remove or disable the access assigned to users of the FABSapplication upon their separation from DISA. Specifically, five FABS application users retainedtheir access past their date of separation. DISA did not remove the users' access until notified bythe auditors that the users had separated.

Cause: DISA's process for removing or disabling FABS application access for users who separate from the agency requires System Administrators to manually remove or disable the users' accounts upon notification of the separation. DISA did not have an effective QC processto ensure System Administrators were notified of all separations and acted to manually remove or disable the access associated with separated users.

Effect: By not removing user access in a timely manner, DISA increases the risk that users mayhave inappropriate access. Additionally, DISA does not have reasonable assurance that it wouldidentify inappropriate access in a timely manner. Furthermore, failing to disable inactive or separated user accounts increases the risk that a compromised user account may be used to perform unauthorized activities.

Recommendations: Kearney recommends that DISA perform the following:

7. Enforce documented policies and procedures in the DISA SD25, *Legacy Mission Applications User Access Desktop Procedures*, regarding account management for the FABS application account removal process.
8. Develop and implement a QC process over the user removal process. The QC process should include procedures to ensure removal of FABS users' accounts after separation.

E. Financial Accounting and Budget System Application Periodic User Access Review

Background: DISA personnel located at FGGM and Scott AFB are responsible for informationsystem security management, including authenticator management for FABS. FABS manages and tracks the financial aspects (e.g., AP, vendor invoices, vouchers) associated with telecommunication circuits, equipment, and services leased from various carriers/vendors on behalf of the Government through the WCF/TSEAS. FABS also supports customer billing, indicating MRCs, non-recurring charges, and overhead charges.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, informs individuals responsible for information systems that periodic review of assigned user privileges is necessary to determine whether the rationale for assigning such privileges remains valid. Periodic review of user accounts is an important security control to ensure only users with the need have the proper privileges in the system. Users may leave the organization, change positions, or acquire new system privileges; therefore, it is important to periodically review system access listings to verify users have only the access and privileges needed to perform their job responsibilities. Unnecessary user access and privileges increase therisk to the confidentiality, integrity, and availability of the system and its data.

Condition: Although DISA had a process to perform periodic access reviews of FABS application accounts, as required by the DoD-wide guidance in FY 2021, personnel who were responsible for completion of the removal of access of users did not do so effectively during theFY 2021 audit cycle. For example, the manner in which the periodic access review was performed revealed inaccuracies in the user listing that were leveraged during the review. In addition, there were some users who were requested by their supervisor to have certain accessesremoved, but those removals were not completed in a timely manner.

Cause: DISA failed to identify inaccurate data initially provided to supervisors for the periodic user access review. DISA's process for performing periodic access reviews of FABS applicationusers included manual actions to initiate and complete the reviews. These actions included the creation of a user listing, which showed user access privileges and was disseminated to their respective supervisors without QC measures in place to ensure the accuracy of the data.
Additionally, DISA failed to confirm the completion of user privilege updates requested by auser's supervisor during the periodic access review.

Effect: By not reviewing accurate user account information, DISA cannot have reasonable assurance that a user's logical account access and level of privileges are appropriate for completing the responsibilities of their assigned role within the application. Additionally, failureto perform a periodic review of accurate information regarding FABS users, as well as the failureto remove unneeded or inappropriate access privileges, increases the risk that fraudulent or erroneous transactions could take place.

Recommendations: Kearney recommends that DISA performs the following:

9. Develop QC procedures to ensure the completeness and accuracy of system-generated user listings used for periodic access review.
10. Ensure actions noted by supervisors as part of the review process are tracked to completion.
11. Maintain evidence of the completed review for third-party verification (i.e., external audit). This evidence should include any actions taken as a result of the review, such as removal of or updates to application accounts.

F. Incomplete Complementary User Entity Control Implementation

Background: DISA utilizes several service organizations to support its operations and mission. As such, DISA obtains assurances from each organization regarding the effectiveness of the organization's internal controls related to the service(s) provided. Specifically, each organization provides a written assertion that accompanies a description of its service(s) and related information system(s). These assertions are communicated via a SOC report. In FY 2021, each service organization provided DISA management with a SOC 1®, Type 2, *Report onan Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, to report on the design and operating effectiveness of its internal controls.

In many cases, service organizations design their controls in support of their service(s) with the assumption that the user entities (i.e., customers or users of the service[s]) will implement certaincontrols (i.e., CUECs) to achieve the overall control objectives and create a secure computing environment. Specifically, the Statement on Standards for Attestation Engagements (SSAE) No.18, *Attestation Standards: Clarification and Recodification*, defines CUECs as controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the service organization's system.

DISA relies on multiple service organizations and their respective SOC reports to gain an understanding of the security posture of each of the systems upon which DISA relies. For example, DISA utilizes the Defense Logistics Agency's (DLA) Defense Agencies Initiative (DAI) system for time and attendance; DLA's Defense Property Accountability System (DPAS)for logistics and property management services; DLA's WAWF for management of goods and services; the Defense Finance and Accounting Service's (DFAS) Defense Cash Accountability System (DCAS) for transaction distribution services; DFAS's Defense Civilian Pay System (DCPS) for Federal civilian payroll services; DFAS's DDRS for financial reporting services; DFAS's Automated Disbursing System (ADS) for standard disbursing services; and the DefenseManpower Data Center's (DMDC) Defense Civilian Personnel Data System (DCPDS) for processing payroll affecting civilian human resource transactions.

Condition: DISA has not implemented all the CUECs required by its service organizations.Based on a subset of high-risk CUECs (i.e., user authorization, periodic access reviews, andseparations) required by DISA's service organizations, examples of control deficiencies indicating CUECs that DISA has not fully implemented included:

- DISA did not maintain adequate documentation to support management's approval of the level of access granted to DISA users of the DPAS application
- DISA did not appropriately authorize users' logical access prior to granting them access to the DCPDS application
- DISA did not perform periodic reviews of DISA users for the WAWF application
- DISA did not document the completion of its periodic review of DISA users for the DCPS application

- DISA did not consistently remove or disable access to DISA users of the DAI and WAWF applications upon their separation from the agency.

Cause: DISA was aware of the requirements for implementing the CUECs and had begun implementation; however, DISA had not finalized its implementation of all CUECs as of the endof fieldwork for the FY 2021 financial statement audit. Throughout FY 2021, DISA performed an internal risk assessment of common CUECs among its service organizations and prioritized testing the implementation of controls it deemed high-risk. While DISA developed test procedures and documented results for each CUEC, it had not documented guidance regarding how it explicitly implemented each CUEC.

Effect: As SOC 1®, Type 2 reports address the effectiveness of controls related to the user entity's financial reporting, ineffective controls or control objectives (e.g., access controls, security management, and configuration management) increase the risk of negative impact to theconfidentiality, integrity, and availability of data supporting DISA's financial statements.
Ineffective controls or control objectives may result from DISA's failure to implement internalcontrols to address all required CUECs.

Recommendations: Kearney recommends that DISA perform the following:

12. Develop a process control document which details how DISA management, system owners, and/or information owners plan to implement all CUECs identified within each service organization's SOC 1®, Type 2 report.
13. Implement all CUECs identified within each service organization's SOC 1®, Type 2 report.
14. Implement a QC review over the CUEC process.

* * * *

KEARNEY& COMPANY

APPENDIX A: STATUS OF PRIOR-YEAR DEFICIENCIES

In the *Independent Auditor's Report on Internal Control over Financial Reporting* included in the audit report on the Defense Information Systems Agency (DISA) Working Capital Fund's (WCF) fiscal year (FY) 2020 financial statements, we noted several issues that were related to internal control over financial reporting. The status of the FY 2020 internal control findings aresummarized in ***Exhibit 3***.

Exhibit 3: Status of Prior-Year Findings

Control Deficiency	FY 2020 Status	FY 2021 Status
Fund Balance with Treasury	Material Weakness	Material Weakness
Accounts Receivable/Revenue/ Accounts Payable/Expense	Material Weakness	Material Weakness
Budgetary Resources	Material Weakness	Material Weakness
Financial Reporting	Material Weakness	Significant Deficiency
Information Technology	Material Weakness	Significant Deficiency

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

INDEPENDENT AUDITOR'S REPORT ON COMPLIANCE WITH LAWS, REGULATIONS, CONTRACTS, AND GRANT AGREEMENTS

To the Director, Defense Information Systems Agency, and Inspector General of the Departmentof Defense

We have audited, in accordance with auditing standards generally accepted in the United Statesof America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; Office of Management and Budget (OMB) Bulletin No. 21-04, *Audit Requirements for Federal Financial Statements*; the Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency(DISA) as of and for the year ended September 30, 2021; and the related notes to the financial statements, which collectively comprise the DISA WCF's financial statements, and we have issued our report thereon dated December 16, 2021.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the DISA WCF's financial statements are free from material misstatement, we performed tests of its compliance with certain provisionsof applicable laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and provisions referred to in Section 803(a) of the Federal Financial Management Improvement Act of 1996 (FFMIA). We limited our tests of compliance to these provisions and did not test compliance with all laws, regulations, contracts, and grant agreements applicable to the DISA WCF. However, providing an opinion on compliance with those provisions was not an objectiveof our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 21-04 and are described in the accompanying Schedule of Findings.

DISA's Response to Findings

The DISA WCF's response to the findings identified in our audit is described in a separate memorandum attached to this report in the Agency Financial Report (AFR). The DISA WCF'sresponse was not subjected to the auditing procedures applied in our audit of the financial statements; accordingly, we express no opinion on it.

KEARNEY&
COMPANY

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's compliance. This report is an integral part of an audit performed in accordance with *GovernmentAuditing Standards* and OMB Bulletin No. 21-04 in considering the entity's compliance.
Accordingly, this communication is not suitable for any other purpose

Alexandria, Virginia
December 16, 2021

KEARNEY& COMPANY

Schedule of Findings

Noncompliance and Other Matters

I. Federal Managers' Financial Integrity Act of 1982 *(Repeat Condition)*

Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, implements the requirements of the FederalManagers' Financial Integrity Act of 1982 (FMFIA). FMFIA and OMB Circular A-123 requireagencies to establish a process to document, assess, and assert to the effectiveness of internal control over financial reporting.

The Defense Information Systems Agency (DISA) has not established or implemented controls in accordance with standards prescribed by the Comptroller General of the United States, as codified in the Government Accountability Office's (GAO) *Standards for Internal Control in theFederal Government* (Green Book), as described by the material weaknesses and significant deficiencies in the *Report on Internal Control over Financial Reporting*.

As discussed in the *Report on Internal Control over Financial Reporting*, the audit identified the following three material weaknesses and two significant deficiencies in internal control which, when aggregated, represent noncompliance with FMFIA and OMB Circular A-123:

Material Weaknesses:
- Fund Balance with Treasury (FBWT)
- Accounts Receivable (AR)/Revenue and Accounts Payable (AP)/Expense
- Budgetary Resources

Significant Deficiencies:
- Financial Reporting
- Information Technology (IT).

II. Noncompliance with the Prompt Payment Act of 1982 *(New Condition)*

DISA is subject to Title 5 of the Code of Federal Regulations (CFR), Section 1315, "The PromptPayment Act." The Prompt Payment Act of 1982 (PPA) generally requires that Federal agenciespay commercial vendors within seven, 10, or 30 days of receipt of a proper invoice, depending on the nature of the product or service being provided. When timely payments are not made, thePPA requires that agencies calculate and include interest penalties in the vendor payments.
Interest penalties represent additional and avoidable costs that decrease the amount of fundsavailable for other needs.

Testing procedures noted violations of the PPA that occurred in the form of untimely payments to vendors, in which the incorrect interest penalty amount was calculated and disbursed. Testingalso noted instances in which the vendors were not paid interest penalties when, in accordance with the PPA, they were due to the vendors. Without a review of all vendor payments, DISA is unable to quantify the total amount of PPA interest due. By not complying with the PPA, DISAincurred additional and avoidable costs in the form of interest penalties. This decreases the amount of funds available for other needs.

DISA Management Comments to Auditor's Report

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

Mr. David Zavada
Kearney & Company
1701 Duke Street, Suite 500
Alexandria, VA 22314

Mr. Zavada:

DISA acknowledges receipt of Kearney & Company's final audit report for DISA's FY 2021 Working Captial Fund (WCF) financial statements.

We acknowledge the auditor-identified findings in the following key areas: 1) Fund Balance with Treasury, 2) Accounts Receivable/Revenue and Accounts Payable/Expense and 3) Budgetary Resources each of which, in the aggregate are considered material weaknesses. We also acknowledge the auditor-identified findings inthe following key areas: 1) Financial Reporting, and 2) Information Technology each ofwhich, in the aggregate are considered significant deficiencies.

DISA has a placed renewed focus on successful resolution of the remaining auditissues during the upcoming audit cycle.

SWONGER.RICHARD.G.[redacted]GREG SWONGER
Digitally signed by SWONGER.RICHARD.G.[redacted]
Date: 2021.12.20 11:25:41 -05'00'

Director, Accounting Operations and Compliance