

**Defense Information Systems Agency
Working Capital Fund
Agency Financial Report
Fiscal Year 2022**



Message From the Defense Information Systems Agency

As the Defense Information Systems Agency (DISA) director, I am presenting the Agency Financial Report (AFR) for the DISA Working Capital Fund (WCF)), as of Sept. 30, 2022. The AFR financial statements and accompanying footnotes incorporate management discussion and analysis, performance, and financial sections that include the auditor's signed report. The AFR is prepared as directed by the Office of Management and Budget Circular A-136.

DISA provides, operates, and assures command, control, and information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support of joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of military operations.

Among DISA's accomplishments in fiscal year 2022, we have continued to provide support to our global Defense Information Systems Network infrastructure, delivering capabilities to our mission partners through desktop and mobile platforms, and leveraging applications hosted at DOD data centers or on commercial clouds. We ensure availability of spectrum through a full range of management activities as well as resiliency and interoperability of our networks and capabilities through net assurance activities and a full range of systems tests and evaluations. DISA plays a role in nearly every combat engagement and supports humanitarian assistance, disaster relief, intelligence, and special operations activities.

The DISA Strategic Plan FY 2022-2024 ensures efforts remain focused toward a shared transparency of understanding so that DISA can achieve the velocity of action needed to win. We are taking bold and decisive action to ensure that the information technology that supports our current and next-generation warfighters and weapons systems are protected from intrusion and attack while creating secure access to critical information — anytime, anywhere.

This year, we have continued to make improvements in our financial processes with oversight by our independent public accounting firm Kearney & Company. DISA can provide reasonable assurance that internal controls over financial reporting, operations, and compliance are operating effectively as of Sept. 30, 2022. We have continued progress addressing significant deficiencies and material weaknesses on DISA's WCF Financial Statements. Information obtained through this year's report and continued improvements leverage our ongoing efforts to improve all aspects of DISA's WCF. The agency continues to improve its posture with a sound internal control environment to execute our strategy effectively while prioritizing command and control, driving force readiness through innovation, and improving cost management.



A handwritten signature in black ink that reads "Robert J. Skinner".

ROBERT J. SKINNER
Lieutenant General, USAF
Director

Table of Contents

Management’s Discussion and Analysis.....	1
Mission and Organizational Structure	2
Performance Goals, Objectives, and Results.....	6
Analysis of Financial Statements and Stewardship Information.....	11
Analysis of Systems, Controls, and Legal Compliance.....	22
Forward-Looking Information.....	34
Principal Statements.....	36
Notes to the Principal Statements.....	41
Required Supplementary Information.....	62
Deferred Maintenance and Repairs Disclosures.....	63
Other Information.....	65
Management Challenges.....	68
Payment Integrity.....	75
DOD Office of Inspector General (OIG) Audit Report Transmittal Letter.....	76
Independent Auditor’s Report.....	80
DISA Management Comments to Auditors Report.....	120

DISA Working Capital Fund Fiscal Year 2022

Management's Discussion and Analysis

The Defense Information Systems Agency (DISA) is pleased to present a Management Discussion and Analysis (MD&A) to accompany its fiscal year (FY) 2022 financial statements and footnotes. The key sections within this MD&A include the following:

- 1. Mission and Organizational Structure**
- 2. Performance Goals, Objectives, and Results**
- 3. Analysis of Financial Statements and Stewardship Information**
- 4. Analysis of Systems, Controls, and Legal Compliance**
- 5. Forward-Looking Information**

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 be the trusted provider to connect and protect the warfighter in cyberspace."

DISA serves the needs of the president, vice president, secretary of defense (SECDEF), Joint Chiefs of Staff (JCS), combatant commands, 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 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.

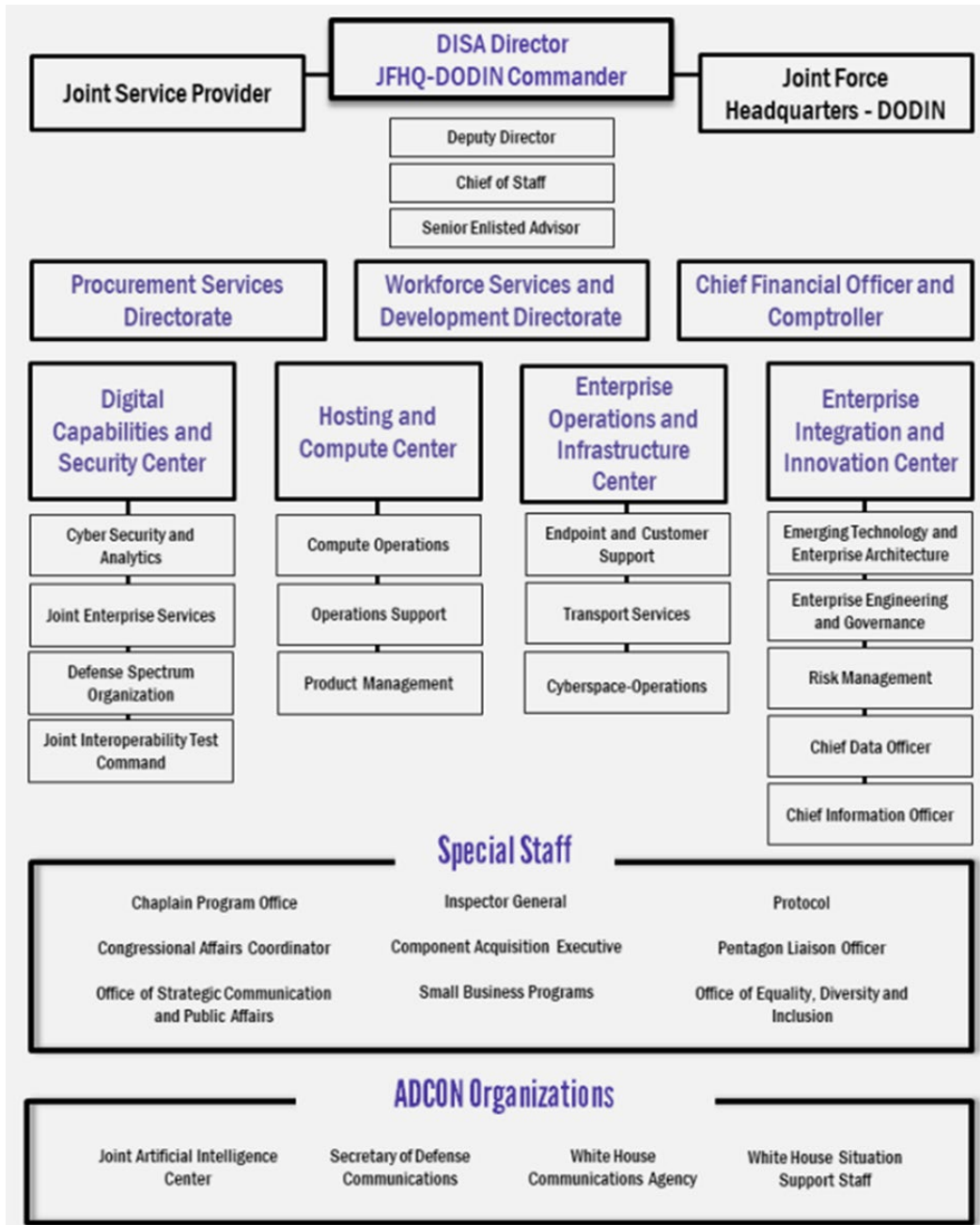
DMRD 918 created the Defense Information Infrastructure (DII) and directed DISA to manage and consolidate the services' and DOD's information processing centers into 16 mega-centers. In FY 2018, the organization that came to be known as the Joint Service Provider (JSP) declared full operational capability 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.



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 September 2022 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 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) (PE55/56). The second component includes Computing Services (CS) (PE54).

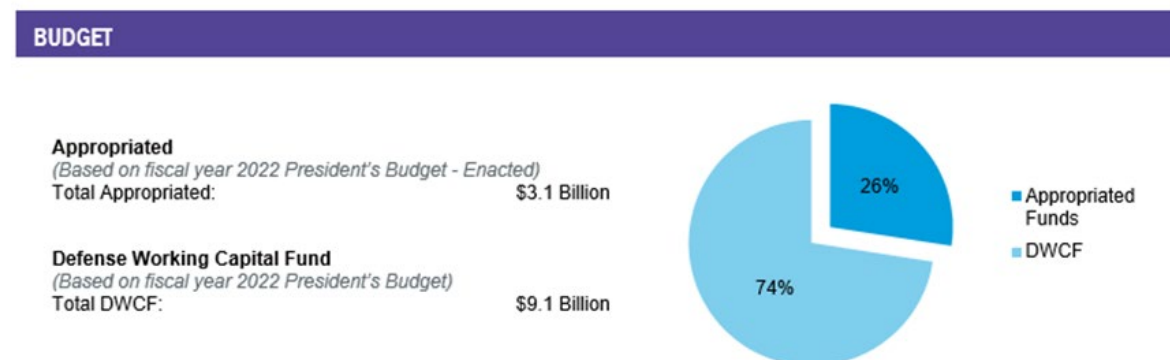
The major element of the Telecommunication Services (TS) component is the Defense Information Systems Network (DISN), which provides interoperable telecommunications connectivity and accompanying services that allow the department to plan and operate both day-to-day business and operational missions 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) (PE56) 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 major programs for DISA WCF are Enterprise Acquisition Services IT Contracts, Joint Enterprise Level Agreements (JELA), Computing Services and Commercial Satellite. Due to normal business operations, major programs may change from year to year.

The Computing Services component of DISA's DWCF activities operates DISA data centers, 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 18 mainframes; more than 16,200 servers; 82,000 terabytes of data; and approximately 260,000 square feet of raised floor.

Resources: DISA is a combat support agency of the DOD with a \$12.2 billion annual budget.



Global Presence

DISA is a global organization of approximately 7,500 civilian employees; 2,000 active-duty military personnel from the Army, Air Force, Navy, and Marine Corps; and over 11,000 defense contractors. This data is as of Sept. 2022. 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 53 percent of its people based at Fort Meade and the National Capital Region, and 47 percent based in field locations.

In addition, the following organizations are a part of DISA: Office of the Chief Financial Officer, Component and Acquisition Executive, Chief of Staff, Inspector General, Joint Force Headquarters- Department of Defense Information Network, Operations and Infrastructure Center, Procurement Services Directorate, Risk Management Executive, White House Communications Agency and Workforce Services and Development Directorate. 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.

Through actions in support of our lines of effort (LOEs), DISA will implement, sustain, and evolve the global network infrastructure and unified capabilities to provide information superiority to the president, the secretary of defense, combatant commanders, senior leadership, military services, defense agencies and the warfighter.

The challenges posed in DISA's strategic objectives are addressed through our LOEs: prioritize command and control, drive force readiness through innovation, leverage data as a center of gravity, harmonize cybersecurity and the user experience, and empower the workforce. Key focus areas throughout these LOEs include improving efficiency and effectiveness, reducing time to deliver solutions, cutting costs, standardizing services, and implementing capability both internally and for our mission partners. New LOEs or actions may be added when necessary to support an agile approach and to achieve our shared vision.

DISA Lines of Effort as outlined in the FY 2022-2024 Strategic Plan include:



The framework addressed through our LOEs — prioritize command and control, drive force readiness through innovation, leverage data as a center of gravity, harmonize cybersecurity and the user experience, and empower the workforce — articulates our vision of a combat support agency that is the nation’s trusted provider to connect and protect the warfighter in cyberspace. We look forward to working with our mission partners, industry, and academia as we continue to strengthen our capabilities and achieve *velocity of action to win*.

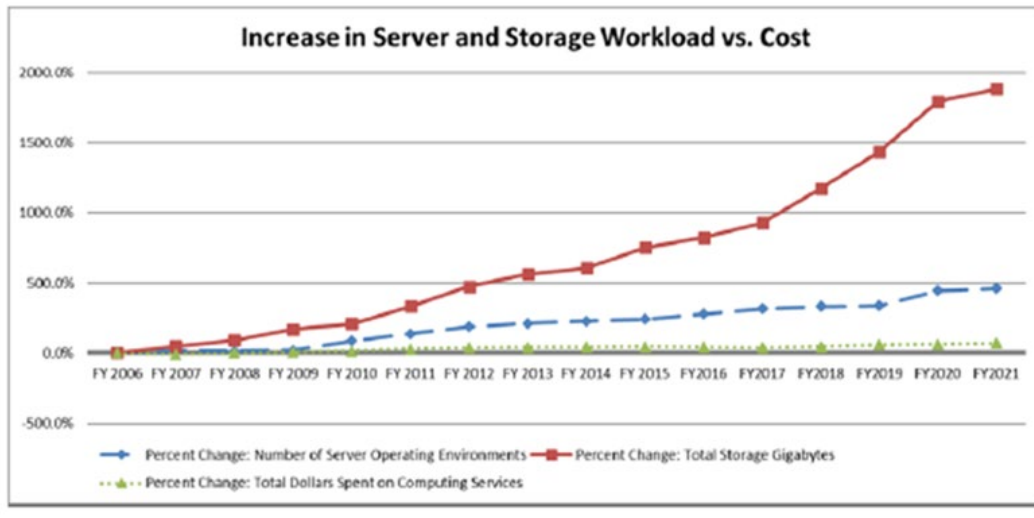
Program Performance

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 with individual customers that exceed the general performance measures discussed in the following paragraphs.

DISA Working Capital Fund (WCF) Performance Measures

The table below represents the increased demand for DISA’s server and storage computing services, which has grown significantly since FY 2006. Since that year, the number of customer-driven server operating environments has increased by 464 percent, and total storage gigabytes have increased by 1,886 percent. Over the same timeframe, the cost to deliver all computing services has increased by only 70

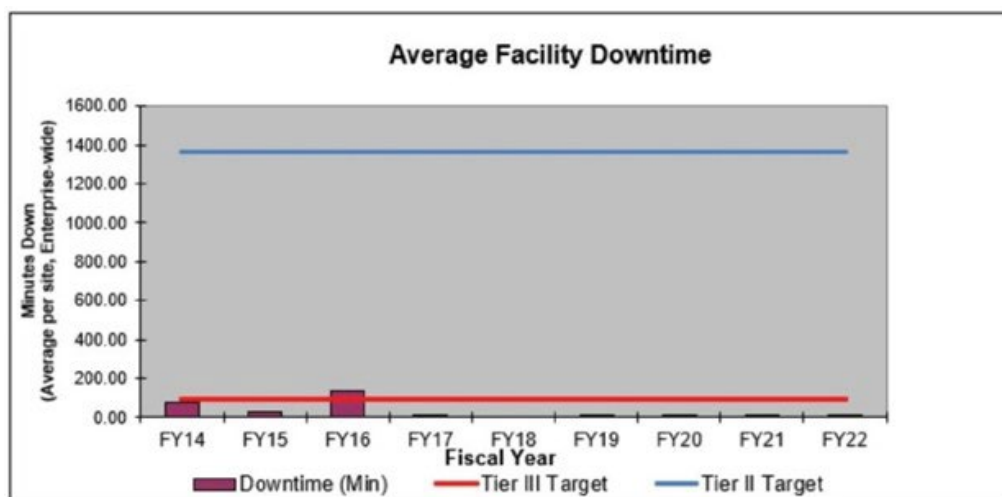
percent. In short, customers are demanding considerably more services and are at the same time benefiting from DISA's unique ability to leverage robust computing capacity at DISA data centers.



The Computing Services 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 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.

Core Data Center Availability



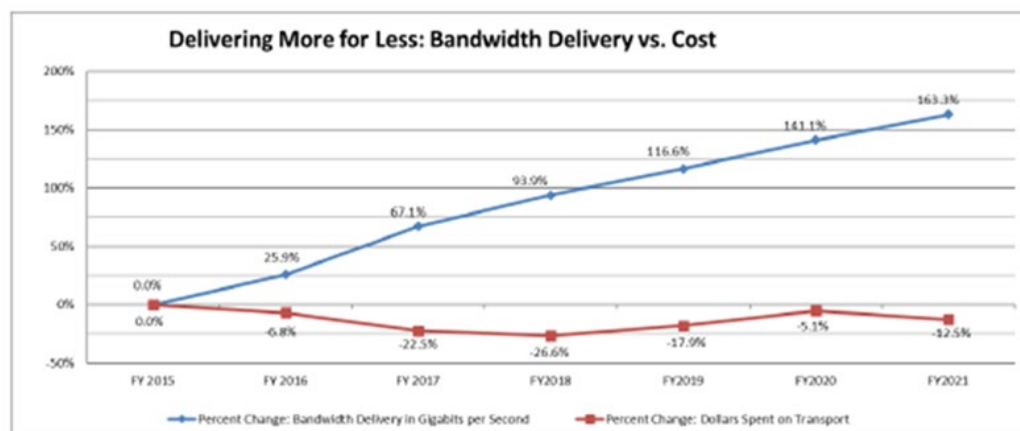
The second metric, "Capacity Service Contract Equipment Availability," represents DISA's equipment availability by technology, i.e., how well DISA is executing its responsibilities exclusive of factors

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.

Figure 1-Capacity Services 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%	99.999%
Communications Devices	99.95%	>99.95%	99.999%

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 connections, with transport costs. Since FY 2015, DISA has increased transport bandwidth delivery capacity 163.3 percent to meet customer demand. The increase is driven by internet traffic, DOD

Enterprise Services, full motion video collaboration, and intelligence, surveillance, and reconnaissance requirements. Over the same timeframe, transport costs associated with the physical connections between sites have decreased by 12.5 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. These categories of metrics have guided the development of the Telecommunication Services budget submission.

Figure 2- Major Performance and Performance Improvement Measures

SERVICE OBJECTIVE	FY 2021 Estimated ACTUAL	FY 2022 Operational Goal	FY 2023 Operational Goal
Non-Secure Internet Protocol Router Network access circuit availability	99.87%	98.50%	98.50%
Secure Internet Protocol Router Network latency (measurement of network delay) in the continental United States	45.23 Milliseconds	<= 100 milliseconds	<= 100 milliseconds
Optical Transport network availability	99.33%	99.50%	99.50%

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 Defense Information Technology Contracting Organization (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 2021 Estimated ACTUAL **	FY 2022 Operational Goal*	FY 2023 Operational Goal*
Percent of total eligible contract dollars completed	80.54%	73.00%	73.00%
Percent of total eligible contract dollars awarded to small businesses	25.29%	28.00%	28.00%

*FY 2022 and FY 2023 goals for percent of total eligible contract dollars completed are estimates based on the released FY 2021 goal. The goals have not yet been released by the Defense Procurement Acquisition Policy (DPAP).

**FY 2021 DISA re-negotiated target to 25%.

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 managers across the agency. This increased focus on accountability for managers has had a significant impact on the critical area of safeguarding assets.

3. Analysis of Financial Statements and Stewardship Information

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 and 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 receive a significant amount of COVID-19-related budgetary resources in FY 2022. DISA WCF does not have any existing indefinite resources associated with COVID requirements. In FY 2022, there was no additional impact to financial reporting for DISA WCF assets, liabilities, cost, revenue, or net position.

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 Status of Fund Balance with the U.S. Department of the Treasury (Line 1.A Unobligated Balance Available, see Footnote 2. FBWT) reflects the results of budget execution that saw the fund increase \$9.4 million for a total of \$107.8 million on its unobligated balance available, as compared with the fourth quarter of FY 2021.

- The Statement of Net Cost reflects a loss through the fourth quarter of FY 2022 of \$90.1 million and includes the non-recoverable depreciation expense for network equipment transferred to DISA WCF (TSEAS-PE55).
- The Statement of Budgetary Resources, New Obligations and Upward Adjustments increased by \$679.2 million, in comparison with the fourth quarter of last year.
- Cash levels remained positive through the fourth quarter of FY 2022 at 12.1 days operating cash.
- Beginning in FY 2020, DISA WCF began budgeting and executing as a "one-fund" entity. In order to reflect 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 being imported into AFS.
- The following analysis of the financial statements presents an explanation of amounts reported in

significant financial statement line items and/or financial notes and variances between the fourth quarter of FY 2022 reported balances and the fourth quarter of FY 2022. 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 (CS and TSEAS). 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 \$187.2 million (67 percent) between the fourth quarter of FY 2021 and the fourth quarter of FY 2022 due to the decrease in earned revenue of \$297.1 million combined with the decrease in gross cost of \$484.3 million between fiscal years.

Figure 4-Net Cost of Operations

(thousands)				
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.
CS	\$ (62,991)	\$ 122,556	\$ (185,547)	-151%
TSEAS	186,845	155,638	31,207	20%
Component	(32,869)	-	(32,869)	-100%
Total	\$ 90,985	\$ 278,194	\$ (187,209)	-67%

Gross Cost - Gross Cost totaling \$7.9 billion increased \$484.3 million (6 percent) between the fourth quarter of FY 2021 and the fourth quarter of FY 2022. In accordance with regulations and guidance, this reflects the full cost of DISA WCF to include recoverable and non-recoverable costs. The primary drivers contributing to the net decrease in gross costs are highlighted in the following table:

Figure 5- Gross Cost

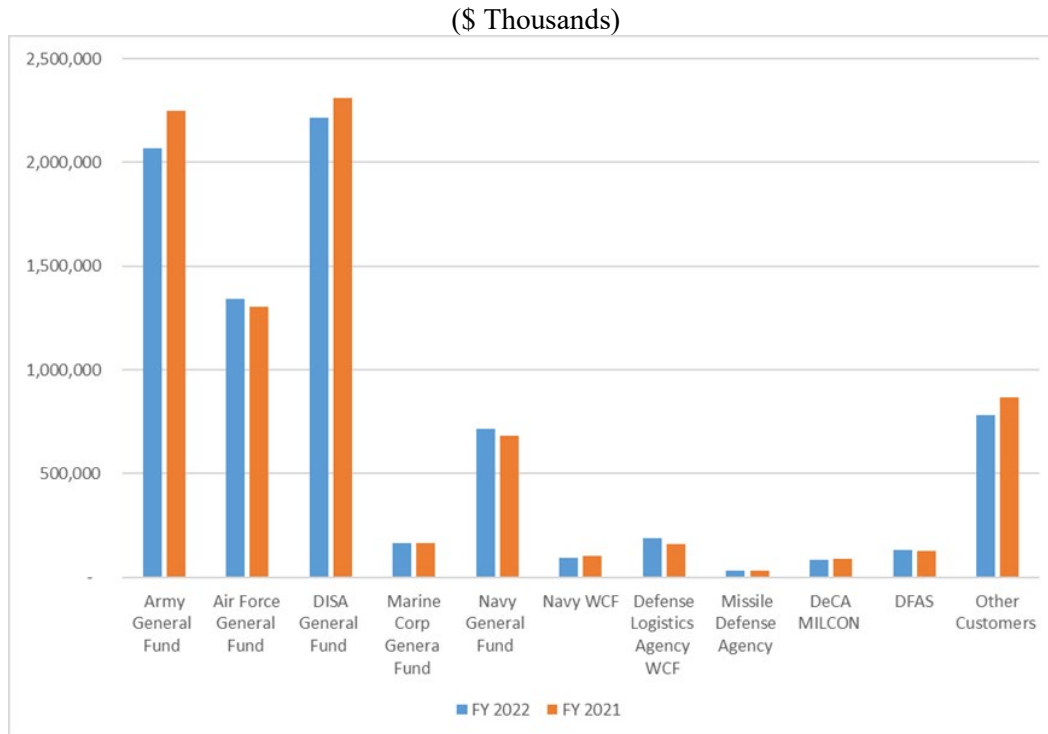
	(thousands)			
DISA WCF (thousands)	9/30/2022	9/30/2021	Inc/Dec	% Chg.
Total Gross Cost	\$7,899,437	\$8,383,736	\$ (484,299)	-6%
Less: PE56 Cost	4,941,758	5,786,284	(844,526)	-15%
Less: Non-Recoverable Depreciation	184,198	171,977	12,221	7%
Total DISA WCF Operating Cost	\$2,773,481	\$2,425,475	\$ 348,006	14%
TSEAS (PE55)				
Bandwidth Management	168,053	210,039	(41,986)	-20%
Enterprise Accounting & Financial Mgmt	74,436	41,801	32,635	78%
Enterprise Internal IT Support	50,913	-	50,913	100%
Transport Capital	28,804	3,987	24,817	622%
CS (PE54)				
Server Systems Administration	37,209	38,206	(997)	-3%
IBM Mainframe Processing	73,692	87,758	(14,066)	-16%
Enterprise Email	45,871	58,947	(13,076)	-22%
Global Service Desk	24,406	43,831	(19,425)	-44%
Component	(44,733)	(942,941)	898,208	-95%
Costs for Remaining Programs	\$2,314,830	\$2,883,847	\$ (569,017)	-20%

*Additional programs added to explain the FY 2022 to FY 2021 variance which changes the cost for remaining programs.

- Non-recoverable depreciation expenses increased \$12.2 million between fiscal years. This increase is a result of more non-recoverable depreciation from the DISA General Fund (GF) without reimbursement in FY 2022 for the transfer-in of general property, plant, and equipment.

Earned Revenue - Earned Revenue totaling \$7.8 billion decreased \$297.1 million (4 percent) between the fourth quarter of FY 2021 and the fourth quarter of FY 2022.

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 2022 and FY 2021.



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

- CS (PE54) Enterprise Email net cost increased \$18.5 million.
- CS IBM Mainframe Processing net cost decreased \$11.9 million.
- CS Global Service Desk net cost decreased \$9.8 million.
- TS (PE55) Enterprise Internal IT Support net cost increased \$50.9 million.
- TS Enterprise Accounting and Financial Management net cost increased \$32.6 million.
- TS Bandwidth Management net cost decreased \$42 million.

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 \$2.1 billion comprise primarily Fund Balance with Treasury (\$338.2 million); Intragovernmental Accounts Receivable (\$735.9 million); and General Property, Plant, and Equipment (PP&E) (\$1 billion).

Fund Balance with Treasury - Fund Balance with Treasury Inception to Date (ITD) Balance increased \$124.6 million 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 2022 and FY 2021, as reflected in the monthly AR(M) 1307 Cash Flow report, presented in a comparative manner:

Figure 6-Fund Balance with Treasury

	(thousands)			
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.
CS Beginning Balance	\$ 31,709	\$ 130,876	\$ (99,167)	-76%
CS YTD	770,038	547,418	222,620	41%
CS Total	801,747	678,294	123,453	18%
TS Beginning Balance	181,944	66,646	115,298	173%
TS YTD	(645,473)	(531,287)	(114,186)	21%
TS Total	(463,529)	(464,641)	1,112	0%
Total Beginning Balance	213,653	197,522	16,131	8%
YTD	124,565	16,131	108,434	672%
Total ITD Balance	\$ 338,218	\$ 213,653	\$ 124,565	58%

- The \$338.2 million cash balance on Sept. 30, 2022, is composed of \$213.7 million current year beginning balance and a FYTD \$124.6 million increase from current year operations (includes capital outlays).
- The current year \$124.6 million increase in fund balance results in a \$161.7 million positive variance when compared with the \$37.1 million forecasted decrease, as reflected in the September 2021 Cash Management Plan. Actual disbursements were \$1.3 billion under plan, and actual collections were \$1.1 billion under plan.
- The WCF increase in cash from operations of \$108.4 million (672 percent) from Sept. 30, 2021, to Sept. 30, 2022, is in line with the decrease in accounts receivable.
- The \$338.2 million WCF inception to date (ITD) cash balance represents approximately 12.1 days of cash on hand on Sept. 30, 2022, which was formulated by dividing \$338.2 million by the daily cash calculation amount of \$27.9 million.
- Amounts recorded in the general ledger for Fund Balance with Treasury (FBWT) have been 100 percent reconciled to amounts reported in the Defense Finance and Accounting Service (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 \$158.5 million (18 percent). The largest decrease was within the TSEAS intragovernmental receivables, primarily from decreases in EAS, Enterprise License Agreements, IT Contracts, and Telecommunications Contracts. This is offset by increases in EAS, Contracting and Acquisition Support, Telecommunication Services, Transport Services, Network Support Services, and Cybersecurity Services.

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

Figure 7-Accounts Receivable, Net

(thousands)					
	9/30/2022	9/30/2021	Inc./(Dec.)	% Chg.	
CS					
Intragov.	\$ 176	\$ 98,664	\$ (98,488)	-100%	
Public	\$ 5	\$ 112	\$ (107)	-96%	
TSEAS					
Intragov.	\$ 735,726	\$ 893,440	\$ (157,714)	-18%	
Public	\$ 942	\$ 878	\$ 64	7%	
Component					
Intragov.	\$ -	\$ (97,700)	\$ 97,700	-100%	
Public	\$ -	\$ -	\$ -	0%	
Total					
Intragov.	\$ 735,902	\$ 894,404	\$ (158,502)	-18%	
Public	\$ 947	\$ 989	\$ (43)	-4%	
Total	\$ 736,849	\$ 895,393	\$ (158,545)	-18%	

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 DISA Computing Ecosystem and TS over the DISN.

Figure 8-General PP&E, Net

(thousands)					
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.	
CS	\$ 17,356	\$ 211,417	\$ (194,061)	-92%	
TSEAS	998,216	696,871	301,345	43%	
Total	\$ 1,015,572	\$ 908,288	\$ 107,284	12%	

- PP&E increased \$107.3 million (12 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 increased \$12.2 million between fiscal years. This increase is a result of more non-recoverable depreciation associated with DISA GF without reimbursement in FY 2022 for the transfer-in of general property, plant, and equipment.

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

Figure 9- PP&E-Net Book Value

	(thousands)			
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.
Net Book Value	\$1,015,572	\$ 908,288	\$ 107,284	
CS PP&E	17,356	211,417	(194,060)	-92%
Joint Regional Security Stacks	198,102	188,575	9,527	5%
Multiprotocol Label Switching	31,256	58,221	(26,965)	-46%
Optical Transport Network	50,016	64,754	(14,738)	-23%
TSEAS DPAS Values	332,259	84,573	247,686	293%
Fiber IRUs	27,408	30,895	(3,487)	-11%
TSEAS Assets Pending	145,324	119,988	25,336	21%
Subtotal	\$ 801,722	\$ 758,424	\$ 43,298	6%
Non-Recoverable Depreciation	184,198	171,977	12,222	7%
Total	\$ 985,921	\$ 930,401	\$ 55,520	6%

Other Assets – Advances and prepayments decreased \$144 thousand (36 percent) within TSEAS and are the result of the current year adjustment to reconcile trading partner data being less than the prior year.

Other Assets balances as of Sept. 30, 2022, and Sept. 30, 2021, are as follows:

Figure 10-Other Assets

	(thousands)			
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.
TSEAS	257	401	(144)	-36%
Total	\$ 257	\$ 401	\$ (144)	-36%

Liabilities

Total liabilities of \$986 million is composed primarily of intragovernmental accounts payable (\$37.9 million), intragovernmental other liabilities (\$2.7 million), non-federal accounts payable (\$894.8 million), other federal employment benefits (\$4.4 million), and non-federal other liabilities (\$45.8 million).

Total Liabilities Not Covered by Budgetary Resources – Total liabilities not covered by budgetary resources decreased \$668 thousand (12 percent) and consisted of other liabilities, military retirement benefits, and the unfunded Federal Employees' Compensation Act (FECA) liability.

Figure 11-Total Liabilities Not Covered by Budgetary Resources

(thousands)					
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.	
CS	\$ -	\$ 3,207	\$ (3,207)	-100%	
TSEAS	5,005	2,466	2,539	103%	
Total	\$ 5,005	\$ 5,673	\$ (668)	-12%	

Total Liabilities Covered by Budgetary Resources – Total liabilities covered by budgetary resources decreased \$57.2 million (6 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 12-Total Liabilities Covered by Budgetary Resources

(thousands)					
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.	
CS	\$ 13,431	\$ 131,155	\$ (117,724)	-90%	
TSEAS	967,519	1,004,695	(37,176)	-4%	
Component	-	(97,700)	97,700	-100%	
Total	\$ 980,950	\$ 1,038,150	\$ (57,200)	-6%	

From a customer funding perspective, DISA GF and Army continue to provide the most customer-funded contract requirements associated with the public accounts payable balance. The decrease in accounts payable is primarily attributed to a decrease in EAS, IT Contracts, offset by increases in Enterprise License Agreements, Transport Services, Delivery Services, and Reimbursable Telecommunication Services. The decrease in CS is due to the One Fund implementation, which took place in October of fiscal year 2021.

Other Liabilities - Other Liabilities decreased \$14.6 million (23 percent), primarily driven by the decrease of accrued funded payroll and leave in CS (\$27.5 million), offset by the increase of accrued funded payroll and leave in TSEAS for \$15.7 million.

Figure 13-Other Liabilities

(thousands)					
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.	
CS					
Intragovernmental	\$ -	\$ 3,300	\$ (3,300)	-100%	
Public	3,706	31,155	(27,449)	-88%	
TS					
Intragovernmental	2,746	2,231	515	23%	
Public	42,060	26,379	15,681	59%	
Total					
Intragovernmental	2,746	5,531	(2,785)	-50%	
Public	45,766	57,534	(11,768)	-20%	
Total Other Liabilities	\$ 48,512	\$ 63,065	\$(14,553)	-23%	

STATEMENT OF CHANGES IN NET POSITION

The Statement of Changes in Net Position presents the change in net position during the reporting period.

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 increased \$83.5 million (72 percent) primarily in Telecommunications Services, specifically Transport Services. This increase is a result of more transfers-in of general property, plant, and equipment along with associated non-recoverable depreciation from DISA GF without reimbursement in FY 2022.
- Imputed financing costs absorbed by others decreased \$33.8 million (59 percent) due to the imputed cost for buildings, which is eliminated for financial reporting purposes.
- Net Cost of Operations decreased \$187.2 million (67 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 United States Standard General Ledger (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 14-Statement of Budgetary Resources

(thousands)					
DISA WCF	9/30/2022	9/30/2021	Inc/Dec	% Chg.	
CS					
Obligations Incurred	\$ (164,459)	\$ 332,733	\$ (497,192)	-149%	
Unobligated Balances	786,711	677,228	109,483	16%	
Contract Authority	(300)	25,995	(26,295)	-101%	
Unfilled Customer Orders	3,273	100,634	(97,361)	-97%	
Net Outlays	(123,452)	(547,418)	423,966	-77%	
TS					
Obligations Incurred	5,474,114	7,681,802	(2,207,688)	-29%	
Unobligated Balances	(678,903)	(549,105)	(129,798)	24%	
Contract Authority	188,381	109,324	79,057	72%	
Unfilled Customer Orders	520,617	2,685,911	(2,165,294)	-81%	
Net Outlays	(1,112)	531,287	(532,399)	-100%	
Component					
Obligations Incurred	2,229,415	(1,154,647)	3,384,062	-293%	
Unobligated Balances	-	(29,759)	29,759	-100%	
Contract Authority	-	-	-	0%	
Unfilled Customer Orders	-	(2,062,895)	2,062,895	-100%	
Net Outlays	-	-	-	0%	
Total					
Obligations Incurred	\$ 7,539,070	\$ 6,859,888	\$ 679,182	10%	
Unobligated Balances	\$ 107,808	\$ 98,364	\$ 9,444	10%	
Contract Authority	\$ 188,081	\$ 135,319	\$ 52,762	39%	
Unfilled Customer Orders	\$ 523,890	\$ 723,650	\$ (199,760)	-28%	
Net Outlays	\$ (124,564)	\$ (16,131)	\$ (108,433)	672%	

New Obligations and Upward Adjustments (line 2190) - Obligations incurred increased \$679.2 million (10 percent). The major drivers for obligations incurred for DISA WCF are as follows:

- The largest increase for Component (DISA99) was due to removing the beginning balance to report One Fund in the WCF instance.
- The DISA WCF incorporated a top-sided adjustment for TSEAS accounts payable/expense and accounts receivable/revenue that affected the obligations incurred for the prior fiscal year. This was done starting in FY 2021 to report corrected comparative numbers.
- The largest decrease for TSEAS was in Enterprise Acquisition Services, IT Contracts, Enterprise License Agreements, and Telecommunications Contracts. There was also an adjustment done to remove the budgetary impact of intra DISA WCF collections and disbursements.
- The largest decreases for CS were in Communication, Overhead, Cloud Services and Enterprise Services, offset by an increase in Server 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, 2022, increased \$9.4 million (10 percent) between fiscal years and is primarily at the Component level due to adjusting the Intra-DISA WCF Business. This is offset by more obligations incurred compared with orders received within CS and TSEAS, specifically in IT Contracts. 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 increased \$52.8 million (39 percent) between fiscal years due to capital investments in the current fiscal year in Transport Services and Cyber Protection Services. In addition, authority for making capital investments in the DISN and cyber capabilities were realigned to the DWCF from appropriated sources.

Unfilled Customer Orders (USSGL 4221) - Unfilled customer orders decreased \$199.8 million (28 percent) between fiscal years 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.

Outlays, Net (Line 4190) - Increased \$108.4 million (672 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.

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. 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.

Figure 15-Net Cost of Operations

(thousands)			
DISA WCF 2022	Intragovernmental	Public	Total
Net Cost of Operations			
Components of Net Cost Not Part of Net Outlays:	\$ (7,380,839)	\$ 7,471,823	\$ 90,983
Property, Plant, and Equipment, net changes	-	107,284	107,284
Increase/(Decrease) in Assets:			
Accounts and taxes receivable, net	(158,508)	(43)	(158,551)
Other Assets	-	(144)	(144)
Increase/(Decrease) in liabilities:			
Accounts Payable	(14,054)	55,648	41,594
Federal employee benefits payable	-	1,635	1,635
Other liabilities	2,928	11,716	14,644
Other Financing Sources:			
Imputed cost	(23,075)	-	(23,075)
Total Components of Net Cost That Are Not Part of Net Outlays	\$ (192,709)	\$ 176,096	\$ (16,613)
Miscellaneous Reconciling Items			
Total Other Reconciling items	(198,938)	-	(198,938)
Total Net Outlays	\$ (7,772,486)	\$ 7,647,919	\$ (124,567)
Agency Outlays, Net, Statement of Budgetary Resources			\$ (124,565)
Unreconciled difference			\$ (2)

*Unreconciled difference is due to rounding.

LIMITATIONS

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.

4. Analysis of Systems, Controls, and Legal Compliance

Management Assurances

DISA Office of the Chief Financial Officer (OCFO)/Comptroller has oversight of DISA's Risk Management and Internal Control (RMIC) Program. Agency assessable unit managers (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 conducts testing and reports on the overall Internal Controls Over Reporting - Financial Reporting (ICOR-FR) for the agency.

Reviews, testing, and evaluations are conducted to assess if the internal control structure is in compliance with the components of the Government Accountability Office (GAO) Green Book objectives of operations, reporting, and compliance. DISA's senior management has reviewed and evaluated the system of internal controls in effect during the fiscal year as of the date of this memorandum, according to the guidance in 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, making adherence of Risk Management and Internal Controls not only the responsibility of management, but also every DISA employee. The concept of reasonable assurance recognizes that DISA's mission objectives are achieved, and managers must carefully consider the appropriate balance among risk, controls, costs, and benefits in our mission-support operations.

Too many controls can result in inefficiencies, while too few controls might increase risk to an unacceptable level. In that premise, 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. 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 reporting, DISA Memo, Annual Statement of Assurance Required Under the Federal Managers' Financial Integrity Act (FMFIA) for FY 2022 operations, and compliance.

Based upon this evaluation, establishing and integrating internal control into its operations in a risk-based and cost beneficial manner, DISA is providing reasonable assurance that our internal controls over reporting, operations, and compliance are operating effectively. Reasonable assurance has been achieved. This position on reasonable assurance is within the limits described in the preceding paragraph.



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

OCT 07 2022

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) 2022

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 one self-reported Material Weakness in SAA activities in FY 2022, reported in the "Significant Deficiencies and Material Weaknesses Template," that internal controls over operations, reporting, and compliance are operating effectively as of September 30, 2022. In FY 2022, there were six categories of material weaknesses (MWs) and Significant Deficiencies (SDs) with the associated Notices of Findings and Recommendations (NFRs) that are in process of correction or have mitigating controls: Accounts Receivable/Revenue (6); Accounts Payable/Expense (11); Budgetary Resources (4); Fund Balance with Treasury (9); Financial Reporting (4); and Information Technology (IT) and Internal Controls (ICs) (9).

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 September 30, 2022.

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.

An evaluation of the internal controls around our SAA activities is limited due to the financial reporting function not yet being 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 that has not been remedied in FY 2022. In FY 2022, DISA has self-reported one MW for Foreign Military Sales cost recovery. Also, from FY 2021 and not fully mitigated in FY 2022, DISA reported one self-identified SD (Government Property in Possession of Contractors) and continues to implement

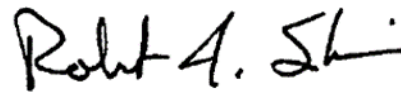
corrective action. There were six categories of MWs with the associated NFRs: Accounts Receivable/Revenue (6); Accounts Payable/Expense (11); Budgetary Resources (4); Fund Balance with Treasury (9); Financial Reporting (4); and IT and ICs (9). Based on the results of the assessment, DISA is able to provide reasonable assurance that internal controls over reporting (including internal and external reporting as of September 30, 2022), and compliance are operating effectively as of September 30, 2022. 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, Federal Financial Management Improvement Act (FFMIA), Section 803, and OMB Circular No. A 123, Appendix D, as of September 30, 2022.

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 that leverage DISA's existing 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 September 30, 2022.

DISA is hereby reporting that no Anti-Deficiency 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 2022, my point of contact is Mr. Alex Diaz, and he can be reached at alexis.diaz20.civ@mail.mil or (614) 692-9400.

A handwritten signature in black ink, appearing to read "Robert J. Skinner".

ROBERT J. SKINNER
Lieutenant General, USAF
Director

Attachments:
As stated

FY 2022 Internal Control Program Initiatives and Execution

In addition to the foundational sources of guidance such as OMB Circular A-123 and the GAO Green Book, DISA also receives direction from and coordinates with the Office of Under Secretary of Defense Comptroller (OUSD [C]) to execute its Risk Management Internal Control (RMIC) Program. The OUSD Comptroller RMIC Team issues the FY 2022 DOD Statement of Assurance Handbook that requires deliverables throughout the reporting cycle. The handbook provides practical guidance to carry out the program. In FY 2022, there was an emphasis on Entity Level Controls (ELCs), auditor Notice of Findings and Recommendations (NFR), Corrective Action Plan (CAP) implementation and resolution, and testing to pave the way in support of CAP resolution or mitigation.

Throughout the process, DISA has provided several templates and deliverables to support not only DISA, but the overall DOD RMIC Program. In the course of the year, DISA will have submitted an End-to-End Process Control Narrative Key Controls Memo, Agency Risk Assessment, Material Weakness (MW) and Deficiencies Reporting and Removal Template, Entity Level Control Testing Validation, Fraud Controls Matrix, Complementary User Control CAPs, Summary of Management's Approach to Internal Control Evaluation Template, and a DATA Act Data Quality Controls Matrix in support of the program.

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 2022, at the time of this memorandum, DISA has a potential to close 16 NFRs upon final review and approval by the independent public accounting firm (IPA).

Entity Level Controls (ELCs):

ELCs 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 emphasizes that there are significant interdependencies among the various control principles. ELCs represent the overarching management controls that create an environment of management oversight for the financial and non-financial activities of the department and DISA as an agency. During the FY 2022 audit, DISA's IPA was briefed on six walkthroughs that outlined 20 different ELCs and provided an overview of the controls that are in place.

Enterprise Approach to Risk Management:

Each year, DISA kicks off its internal control program and begins by performing a risk assessment in which 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 of "undergo an audit and improve the quality of budgetary and financial information that is most valuable in managing the DOD," through its audit and environment of continuous improvement and process refinement. 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, which 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, within each assessable unit, collaborates with AUMs to identify areas of risks in their respective area. The processes of coordinating and consolidating risk help identify the overall assessment of risk at the enterprise risk management level, while also reviewing DISA's detail transactions. This risk assessment results in reviews and letters of assurance from each area that are considered in the annual Statement of Assurance assessment.

Oversight and Monitoring:

DISA's internal control structure of training provides AUM assistance; ELCs; risk assessments; continuous testing in mandatory and high-risk areas; reviews, updates, and management approval of process narratives and cycle-memos; CAPs; and senior accountable officials (SOAs) letters of assurance. These elements are all core to an integral program of oversight and monitoring. In addition, the Senior Assessment Team (SAT) met on Aug. 9, 2022, and provided oversight to the internal control program through discussion of results and anticipated outcomes to be reported in the FY 2022 Statement of Assurance.

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, DFAS, as DISA's accounting service provider, performs overpayment recapture functions on behalf of DISA. DFAS includes DISA transactions in its sampling populations for improper payment testing of civilian payroll and travel. There have been no issues arising to merit an anticipated DISA Memo, Annual Statement of Assurance Required Under the FMFIA for FY 2022 negative impact regarding payment integrity and improper payment recovery in FY 2022.

CARES Act/COVID-19:

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed on March 2, 2020, (Public Law 116-136) and includes a military support response to the public health emergency domestically and internationally. Since FY 2021, DISA has been allotted \$182.9 million in CARES Act cumulative 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 2022. Identified areas of improvements for CARES Act execution include ensuring DISA Memo, Annual Statement of Assurance Required Under the FMFIA for FY 2022 requirements are aligned with spending plans and ensuring that transactions accurately reflect the Disaster Emergency Fund Code (DEFC).

Fraud Controls:

In FY 2022, DISA executed a fraud controls assessment on its environment. The review incorporated components of GAO Fraud Risk Management Framework 11 leading practices to detect gaps that require designing new or additional controls. These practices were employed in review of ICOR-O, ICOR-FR,

and ICOR-FS for high-risk focus areas.

End-to-End Process Control Narrative (PCN) Memo:

One of the new requirements in FY 2022 was completion of the End-to-End Process Control Key Controls Memorandum. DISA completed a review and assessed that our narratives and key controls do not depart from the key controls at the DOD-wide level. Our DISA general roles and functions as presented in our narratives and cycle memos correlate with DOD-wide key controls. These include civilian payroll, requisitioning, contract and vendor pay, general property plant and equipment, and reimbursable work orders.

Security Assistance Agency (SAA)/Foreign Military Sales (FMS):

DISA is an implementing agency (IA) that supports the execution of military assistance programs. As an IA, DISA 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 participating in DSCA's preparation for auditable financial statements. As of this fiscal year, DISA is not performing the financial reporting function for DSCA; however, the internal control structure already in place for DISA's General Fund and WCF audits are leveraged for the FMS process.

Although SAA internal controls reviews are not new, the FY 2022 requirement to review the cost recovery structure has been initiated in FY 2022. The DOD Inspector General issued a report (DODIG-2020-114) on the DOD's use of Security Assistance Funds and Asset Accountability. The report determined that DOD components did not recover their costs for executing security assistance programs in accordance with the Arms Export Control Act and the DOD Financial Management Regulation. Specifically, the DOD components did not recover their costs for paying DOD civilians to work on the security assistance programs. We performed a cost recovery review that documents that FMS personnel, aligned with FMS-related functions, are being paid with FMS dollars; however, non-FMS personnel are not being paid with FMS dollars. This finding has resulted in a MW and non-compliance with the principle that FMS business be conducted at no cost to the U.S. government. A plan has been put in place to ensure all FMS activity is captured and covered by FMS funding.

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) Act. 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 2022, in compliance with mandatory reviews, the internal control program has executed data quality testing to review data integrity. Testing results have documented that there are no major issues with the established attributes in both fiscal years 2021 and 2022.

Records Management:

While records management was not an OUSD focal area, the DISA Records Management team and the Internal Control team coordinated together to incorporate a records management checklist into their processes. The results supported that DISA has established 100 percent coverage and accountability throughout the organization with appointments of Records Liaisons (RLs). As an agency, we have completed the 2021 Records Management Self-Assessment (RMSA) for the National Archives and Records Administration (NARA) and improved the agency's score. We have also completed the 2021 Federal Electronic Records and Email Management Maturity Model Report (FEREM) for NARA and taken the agency from a moderate to a low risk.

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 that defines management’s leadership and commitment towards an effective RMIC: openness, honesty, integrity, and ethical behavior. The memo directed the agency to follow 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 throughout DISA 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 OUSD comptroller regarding the RMIC Program, in addition to providing training, guidance, oversight, and review in accordance with directives to the AUMs. DISA provided internal control kick-off training for the AUMs in November 2021 and conducted three additional workshops in the FY 2022 reporting cycle to address risk assessments, testing grids, and letters of assurance. The RMIC team compiles assessable unit (AU) submissions for the agency’s Statement of Assurance, facilitates information sharing between AUMs, consolidates results, and communicates outcomes to OUSD and agency leadership.

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 13 AUs:

- ✓ Chief Financial Officer/Comptroller (OCFO)
- ✓ Component and Acquisition Executive (CAE)
- ✓ Digital Capabilities and Security Center (DCSC)
- ✓ Chief of Staff (DDC)
- ✓ Inspector General (IG)

Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN)

- ✓ Joint Service Provider (JSP)
- ✓ Hosting and Compute Center (HaCC)
- ✓ White House Situation Room (WHSR)
- ✓ Procurement Services Directorate (PSD)
- ✓ Enterprise Integration and Innovation Center (EIIC)
- ✓ 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.

In the first quarter FY 2022, DISA experienced a reorganization that impacted organizational lines. The Internal Control Office reached out to the impacted areas and identified gaps in reporting that mainly impacted operations activities, which had been absorbed into different areas. AUs shared responsibility at the center level to include those areas in mandatory testing.

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 property, plant, and equipment (PP&E) to identify the level of process documentation available and determine the associated risk of those functions. Additionally, AUMs are responsible for identifying and documenting the key controls within their AUs in accordance with DOD Instruction 5010.40. The internal control team documents processes and key controls for all ICOR-FR functions through detailed cycle memoranda and narratives. Each AU documents its key processes and risks on the Risk Assessment Template. The OCFO RMIC team advises 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. In addition, a checklist for records management was prepared by each AUM.

Assessable Unit manager (AUM) Risk Assessment Template Excerpt

		Risk Ranking			Risk Management and Risk Response				Residual Risk			
Risk Owner	Process Owner	Overall Impact	Overall Likelihood	Overall Risk Ranking	Current Risk Response	Control Activities	Control Effectiveness	Risk Appropriately Mitigated?	Residual Risk Description	Overall Residual Risk Impact	Overall Residual Risk Likelihood	Overall Residual Risk Ranking
Test	Test	Based on factors including financial impact, reputational impact, and operational impact: -High -Medium -Low	Based on Probability and Frequency: - High - Medium - Low Dropdown	Based on a function of overall likelihood and overall impact: -High: the risk is very likely or reasonably expected to occur; -Medium: the risk is more likely to occur than unlikely; and -Low: the risk is unlikely to occur. Dropdown	The action taken to manage the risk. It could involve one or more of the following: -Acceptance -Avoidance -Reduction -Sharing (Transferring) Dropdown	Description of the Control Activities Text	1: Implemented & effective 3: Partially implemented and/or effective 5: Do not exist or are not implemented Dropdown	Dropdown	Text	Based on factors including financial impact, reputational impact, and operational impact: -High -Medium -Low Dropdown	Based on Probability and Frequency: - High - Medium - Low Dropdown	Based on a function of overall likelihood and overall impact: -High: the risk is very likely or reasonably expected to occur; -Medium: the risk is more likely to occur than unlikely; and -Low: the risk is unlikely to occur

Each AU performs a risk assessment considering what is important to each area, such as those processes that may be high or medium risk and associated processes that are central to an area. It involves identifying the risk category (e.g., financial, compliance, operational, etc.); risk description (e.g., if policy is not implemented); overall impact, likelihood, risk rating, and control activities (such as review and documented policy); whether risks are mitigated or residual; overall likelihood; and residual risk rating, process documentation, and financial statement impact. At the AU level and across the agency, this process develops an overarching risk assessment, approved by senior leadership. From this process, tests are developed for those areas that are high risk or into which management should look further.

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 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:									
Process Name:		Directorate/Org:									
Narrative Reference:		Preparer Name:									
Objective Type:	Reporting	Preparer Phone:									
Risk Type:	Inherent										
Risk Response:	Reduce										
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.

Test Results

After the tests are conducted and results are revealed, the test grid forms the basis to report the results in the letter of assurance (LoA). The LoA will reflect the data reported on the test grid.

Letter of Assurance (LoA)

Internal Control Currently in Place (Control Objective)	Control Criteria	Control Type	Control Frequency	Tolerance Rate	Test Plan (Description)	Test Type	Sample Size	Summary of Test Results	Significant Deficiency?	Material Weakness?

A. Travel (DTS):

- a. Describe how your organization conducted testing (consider the nature, extent including sampling technique) and timing of the execution of the control tests:
- b. Did you use a checklist?
- c. Test method (inquiry, observation, inspection, or re-performance):
- d. Sample size/sampling technique/tolerance rate:
- e. Describe control(s):
- f. Summarize test results:
- g. Describe any findings, significant deficiencies or material weaknesses:
- h. If any significant deficiencies or material weaknesses were identified, was a Corrective Action Plan (CAP) prepared?
- i. Level of Assurance (unmodified, modified, or no assurance):

Snapshot in Review

Internal Controls Over Reporting - Operations

Mandatory testing is required for all organizations. In coordination with senior management, AUMs identify 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. Government Purchase Card and Records Management are 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

The implementation of Enterprise Resource Planning (ERP) approved systems as of FY 2019 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 anti-deficiency 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 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: the Defense Finance and Accounting Service (DFAS), the Defense Logistics Agency (DLA), the Defense Contract Management Agency (DCMA), the Defense Human Resource Activity (DHRA), military services, and other defense organizations. As a result, DISA is responsible for most of the general IT controls over the computing environment in which many financial, personnel, and logistics applications reside. For service providers and components to rely on automated controls and documentation within these applications, controls must be appropriately and effectively designed. In FY 2022, 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 a modified opinion for hosting 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 analyses of the results of financial operations, and known upcoming business events. An internal control assessment was conducted within DISA for key mission-specific processes. The internal control team annually reviews and updates narratives and cycle memos of key processes. The internal control team maintains a Control Evaluation Matrix, which provides a detailed analysis, documents the Control Activities identified in the narratives, and includes mapping to a Financial Improvement and Audit Readiness (FIAR) Financial Reporting Objective; FIAR Risk of Material Misstatement, Test of Design and Implementation Effectiveness details; and test of Operating Effectiveness details.

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:

Figure 16-Areas of Testing

General Fund	Working Capital Fund	Other
Data Quality Plan	CS Trial Balance (Rollforward) Testing	Active Users
Dormant Reviews*	TSEAS Trial Balance (Rollforward) Testing	Departed Users*
Year End Obligations	TSEAS Revenue	Security Awareness Training
Trial Balance Rollforward Testing	TSEAS Expenditure	Segregation of Duties
GF Revenue		PP&E Additions
GF Expenditure		PP&E Disposals
CARES Act Testing*		Periodic Access Systems Review*
Accounts Receivable Reporting		
FMS Cost Recovery		

*Exceptions of non-compliance.

The OUSD Financial Improvement and Audit Readiness (FIAR) Office led department-wide discussions regarding SSAE 18 reviews and the impact to component financial statements. DISA identified more than 201 Complementary User Entity Controls (CUECs) that impacted 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 201 identified CUECs to determine our level of risk and identified control descriptions and attributes for each. For those CUECs determined to be common across all the identified systems, testing was conducted for areas of high risk. In addition, the internal control team has developed active and departed user segregation of duties and periodic access system reviews to a more granular level. Review of these areas further strengthens the internal control backbone for the agency.

The following tables provides a summary of DISA's approach to the FY 2022 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:

- Chief Financial Officer/Comptroller (OCFO)
- Component and Acquisition Executive (CAE)
- Digital Capabilities and Security Center (DCSC)
- Chief of Staff (DDC)
- Inspector General (IG)
- Joint Force Headquarters DODIN (JFHQ-DODIN)
- Joint Service Provider (JSP)
- Hosting and Compute Center (HACC)
- White House Situation Room (WHSR)
- Procurement Services Directorate (PSD)
- Enterprise Integration and Innovation Center (EIIC)
- White House Communications Agency (WHCA)
- Workforce Services and Development Directorate (WSD)

List of all Component material AUs related to ICOR

- Chief Financial Officer/Comptroller (OCFO)
- Hosting and Compute Center (HACC)
- Procurement Services Directorate (PSD)

Summary of Internal Control Evaluation Approach: DISA's approach to internal controls extends to all responsibilities and activities undertaken within DISA. Adherence of RMIC Program internal controls is not only the responsibility of Management, but every DISA employee. In addition to compliance with applicable laws and regulations, internal controls are embedded in DISA's day to day processes. Internal controls have been evaluated in a top down and bottom-up approach resulting in reasonable assurance that financial reporting, operations, and systems are operating effectively.

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	Yes
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-Overall Evaluation of a System of Internal Control

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

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 DOD, which facilitates 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 2022, DISA continued to operate, enhance, and sustain the Financial Accounting and Management Information System (FAMIS), which supports the full breadth of DISA's WCF lines of business. The FAMIS-WCF solution provided DISA with DOD Standard Line of Accounting (SLOA) and USSGL compliance in support of a clean audit opinion for the WCF. Additionally, FY 2022 activities/goals include performing a technology refresh of the FAMIS software; implementing a compliant G-invoicing solution; completing Phase II of Direct Treasury Disbursing; implementing SOA/Web Services capabilities; and laying the groundwork to migrate FAMIS to a commercial cloud environment. 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 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 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.

In that regard, DISA is driving standardization of the customer order provisioning process to include a single integrated order entry solution for all orders while validating the solutions that integrate with DISA's financial and contracting systems and tools. DISA's financial systems strategy is purpose driven to continually innovate and increase its use of technologies, such as robotic process automation and 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 three years, its accounting operations have stabilized, and it is taking advantage of its 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 will result in increased automation, transparency, access, and control of financial information to support financial managers, mission partners, and higher echelon leaders.

5. Forward-Looking Information

The DOD information environment is designed to optimize the 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 DOD information environment through the development, integration, and synchronization of 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 Joint Information Environment, DISA data centers have been identified as continental United States (CONUS) Core Data Centers.

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:

- 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.
- The delivery of an on-premises, cloud hosting capability and commercial cloud access infrastructure 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 Compute Operations (formerly 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 Compute Operations prioritizes excellence in service delivery, process efficiency, and standardization for tools and processes. Ultimately, the shift to the Compute Operations 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.

**Defense Information Systems Agency
Working Capital Fund
Principal Statements
Fiscal Year 2022, Ending Sept. 30, 2022**

Department of Defense
Defense Information Systems Agency WCF
As of Sept. 30, 2022 and 2021
(\$ in thousands)

Figure 19-Balance Sheet

	<u>2022</u>	<u>2021</u>
Intragovernmental assets:		
Fund Balance with Treasury (Note 2)	\$ 338,218	\$ 213,653
Accounts receivable, Net (Note 3)	735,901	894,403
Total Intragovernmental Assets	1,074,119	1,108,056
Other than intragovernmental assets:		
Accounts receivable, net (Note 3)	947	990
General property, plant and equipment, net (Note 4)	1,015,572	908,288
Advances and prepayments	257	401
Total other than intragovernmental assets	1,016,776	909,679
Total Assets	\$ 2,090,895	\$ 2,017,735
Liabilities (Note 7)		
Intragovernmental liabilities:		
Accounts payable	\$ 37,920	\$ 23,860
Advances from others and Deferred Revenue (Note 7)	257	401
Other Liabilities (Notes 7 and 9)	2,746	5,531
Total intragovernmental liabilities	40,923	29,792
Other than intragovernmental liabilities:		
Accounts payable	894,830	950,477
Federal employee and veteran benefits payable (Note 6)	4,376	6,011
Advances from Others and Deferred Revenue (Note 7)	59	7
Other Liabilities (Notes 7, 8 and 9)	45,766	57,534
Total other than intragovernmental liabilities	945,031	1,014,030
Total liabilities	985,954	1,043,822
Commitments and contingencies (Note 9)		
Net Position:		
Cumulative Results from Operations	1,104,941	973,913
Total Cumulative Results of Operations (Consolidated)	1,104,941	973,913
Total net position	1,104,941	973,913
Total liabilities and net position	\$ 2,090,895	\$ 2,017,735

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

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2022 and 2021
(\$ in thousands)

Figure 20-Statement of Net Cost

Gross Program Costs (Note 10, Note 12, Note 14)	<u>2022</u>	<u>2021</u>
Gross Costs (Note 10, Note 12)	\$ 7,899,436	\$ 8,383,736
Less: Earned Revenue (Note 11)	(7,808,451)	(8,105,542)
Net Cost of Operations	90,985	278,194
Enterprise Acquisition Services	168,053	210,039
Commercial Satellite	74,436	41,801
Bandwidth Management	73,692	87,758
Enhanced Mobile Satellite Services	50,913	-
Other Programs	7,532,343	8,044,138
Less: Earned Revenue	(7,808,452)	(8,105,542)
Net Other Program Costs	\$ 90,985	\$ 278,194

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

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2022 and 2021
(\$ in thousands)

Figure 21-Statement of Changes in Net Position

CUMULATIVE RESULTS OF OPERATIONS	<u>2022</u>	<u>2021</u>
Beginning Balance	\$ 973,913	\$1,079,789
Non-exchange revenue	-	-
Transfers-in/out without reimbursement	198,938	115,419
Imputed financing	23,075	56,900
Other	-	(1)
Net Cost of Operations	90,985	278,194
Net Change in Cumulative Results of Operations	131,028	(105,876)
Total Cumulative Results of Operation	1,104,941	973,913
Net Position	\$1,104,941	\$ 973,913

Department of Defense
Defense Information Systems Agency WCF
For the Years Ended Sept. 30, 2022 and 2021
(\$ in thousands)

Figure 22-Statement of Budgetary Resources

	<u>2022</u>	<u>2021</u>
Budgetary Resources		
Unobligated balance from prior year budget authority, Net (Note 12)	\$ 98,506	\$ 358,978
Contract Authority (discretionary and mandatory)	188,081	135,319
Spending Authority from offsetting collections (discretionary and mandatory)	7,360,290	6,463,955
Total Budgetary Resources	<u>7,646,877</u>	<u>6,958,252</u>
Status of Budgetary Resources		
New obligations and upward adjustments (total)	7,539,069	6,859,888
Unobligated balance, end of year		
Apportioned, unexpired accounts	107,808	98,364
Unexpired unobligated balance, end of year	<u>107,808</u>	<u>98,364</u>
Unobligated balance, end of year (total)	<u>107,808</u>	<u>98,364</u>
Total Budgetary Resources	<u>7,646,877</u>	<u>6,958,252</u>
Outlays, Net		
Outlays, net (total) (discretionary and mandatory) (Note 13)	<u>(124,564)</u>	<u>(16,131)</u>
Agency Outlays, net (discretionary and mandatory)	<u>\$ (124,564)</u>	<u>\$ (16,131)</u>

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

**Defense Information Systems Agency
Working Capital Fund
Notes to the Principal Statements
Fiscal Year 2022, Ending Sept. 30, 2022**

DEFENSE INFORMATION SYSTEMS AGENCY
WORKING CAPITAL FUND

Notes to the Principal Statements
Fiscal Year 2022, Ending Sept. 30, 2022

Note 1. Summary of Significant Accounting Policies

1A. Reporting Entity

DISA, a combat support agency within the DOD, is a component reporting entity, as defined by the Statement of Federal Financial Accounting Standards (SFFAS) 47, and its financial statements are consolidated into those of the DOD. These 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.

The DOD includes the Office of the Secretary of Defense (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 of the DOD AFR provides a list of the components, which comprise 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 of 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.

DISA WCF does not meet the SFFAS 47 criteria to include disclosure entities with any ownership interest, financial exposure, or potential impact of the relationship on reported financial relationship in its WCF financial statement notes.

1B. Accounting Policies

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 have 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	\$ -	\$ 8,273
2110-Accounts Payable	Credit	8,273	-
4210-Anticipated Reimbursements	Debit	-	-
4221-Unfilled Customer Orders without Advance	Debit	-	44,911
4251-Reimbursements and Other Income Earned- Receivable	Debit	-	8,273
4590-Appportionments	Credit	-	-
4610-Allotments-Realized Resources	Credit	-	17,756
4700-Commitments	Credit	-	637
4801-Undelivered Orders-Obligations, Unpaid	Credit	63,304	-
4871-Downward Adjustments of prior year Unpaid UDOs	Debit	-	-
4901-Delivered Orders-Obligations, Unpaid	Credit	8,273	-
5200-Revenue	Credit	30,634	-
6100-Expense	Debit	-	30,634

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

(thousands)

	Normal D/C	Debit Amount	Credit Amount
4902-Deliverd Orders-Obligations, Paid	Credit	\$ 131,971	\$ -
4252-Reimburseemnts and Other Income Earned- Collected	Debit	-	131,971

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. DISA WCF presents the Balance Sheet, Statement of Net Cost, and Statement of Changes in Net Position which 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, intragovernmental activity has not been eliminated. The intra-DISA WCF balances for outlays and collections business between the Telecommunication Services Enterprise Acquisition Services (TSEAS) and Computing Services (CS)

business components have been removed from the Statement of Budgetary Resources (SBR).

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.
- 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 Office of Management and Budget (OMB) Circular No. A-136 and U.S. Generally Accepted Accounting Principles (GAAP).

1C. Fund Balance with Treasury

The Fund Balance with Treasury (FBWT) represents the aggregate amount of 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 Defense Finance and Accounting Service (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 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 General Fund. In both cases, the amounts represent commitments by the government to provide resources for programs, but they do not represent net assets to the government as a 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 by appropriation on interagency transfers, collections received, and disbursements issued. 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. The FBWT 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.

DISA Working Capital Fund FBWT balance is reconciled monthly to the amounts reported in the Cash Management Report (CMR), which represents DISA's portion of the FBWT balance reported by the Treasury Department. The settlement process incorporates a baseline reconciliation performed during FY

2005. The baseline reconciliation includes activity from the revolving fund's inception in FY 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 *Fund Balance with Treasury Note 2* below.

1D. 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 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 7 "Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting," 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. 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 that 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.

1E. Budgetary Terms

The purpose of federal budgetary accounting is to control, monitor, and report on funds made available to federal agencies by law and help ensure compliance with the law.

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 following budgetary terms are commonly used:

- Appropriation is a provision of law (not necessarily in an appropriations act) authorizing the expenditure of funds for a given purpose. Usually, but not always, an appropriation provides budget authority.
- Budgetary resources are amounts available to incur obligations in a given year. Budgetary resources consist of new budget authority and unobligated balances of budget authority provided in previous years.
- Obligation is a binding agreement that will result in outlays, immediately or in the future. Budgetary resources must be available before obligations can be incurred legally.
- Offsetting Collections are payments to the government that, by law, are credited directly to expenditure accounts and deducted from gross budget authority and outlays of the expenditure account, rather than added to receipts. Usually, offsetting collections are authorized to be spent for the purposes of the account without further action by Congress. They usually result from business-like transactions with the public, including payments from the public in exchange for goods and services, reimbursements for damages, and gifts or donations of money to the government and from intragovernmental transactions with other government accounts. The authority to spend collections is a form of budget authority.
- Offsetting receipts are payments to the government that are credited to offsetting receipt accounts and deducted from gross budget authority and outlays, rather than added to receipts. Usually, they are deducted at the level of the agency and subfunction, but in some cases they are deducted at the level of the government as a whole. They are not authorized to be credited to expenditure accounts. The legislation that authorizes the offsetting receipts may earmark them for a specific purpose and either appropriate them for expenditures for that purpose or require them to be appropriated in annual appropriations acts before they can be spent. Like offsetting collections, they usually result from business-like transactions with the public, including payments from the public in exchange for goods and services, reimbursements for damages, and gifts or donations of money to the government, and from intragovernmental transactions with other government accounts.
- Outlays are the liquidation of an obligation that generally takes the form of an electronic funds transfer. Outlays are reported both gross and net of offsetting collections and they are the measure of government spending.

For further information about budget terms and concepts, see the “Budget Concepts” chapter of the *Analytical Perspectives* volume of the President’s Budget: [Analytical Perspectives | The White House](#).

1F. Changes in Entity or Financial Reporting

Due to a change in methodology to calculate depreciation and capitalized expenditures, 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.

1G. Classified Activities

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

Note 2. Fund Balance with Treasury

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 \$107.8 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 \$1.5 billion represents funds obligated for goods and services but not paid.

The Non-FBWT budgetary accounts in the amount of \$1.3 billion reduce budgetary resources and are primarily composed of unfilled customer orders without advance from customers in the amount of \$523.9 million, contract authority in the amount of \$227 million, and receivables and other in the amount of \$543 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 provides 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 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 the 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 25-Fund Balance with Treasury

(thousands)		
DISA WCF	<u>2022</u>	<u>2021</u>
Unobligated Balance:		
Available	\$ 107,808	\$ 98,364
Total Unobligated Balance	<u>107,808</u>	<u>98,364</u>
Obligated Balance not yet Disbursed	1,524,266	1,834,349
Non-FBWT Budgetary Accounts:		
Unfilled Customer Orders without Advance	(523,890)	(723,650)
Contract Authority	(226,977)	(192,841)
Receivables and Other	(542,989)	(802,569)
Total Non-FBWT Budgetary Accounts	<u>(1,293,856)</u>	<u>(1,719,060)</u>
Total FBWT	<u>\$ 338,218</u>	<u>\$ 213,653</u>

Note 3. Accounts Receivable, Net

Accounts receivable represent 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 doubtful accounts (estimated uncollectible amounts) due are based on an analysis of aged accounts receivable. DISA analyzes intragovernmental allowances based on individual receivable transactions aged greater than two years to determine their collectability and potential inclusion in our quarterly allowance journal voucher. DISA also includes receivable transactions aged less than two years if doubts about collectability have been identified. The non-federal accounts receivable allowance is calculated based on the prior month's average uncollected individual debt greater than 91 days as reported in the Treasury Report on receivables and the monthly receivables report from the Defense Debt Management System (DDMS).

Figure 26-Accounts Receivable, Net

(thousands)			
DISA WCF 2022	Gross Amount Due	Allowance for Estimated Uncollectibles	Accounts Receivable, Net
Intragovernmental Receivables	\$ 739,184	\$ (3,282)	\$ 735,902
Non-Federal Receivables (From the Public)	949	(2)	947
Total Accounts Receivable	\$ 740,133	\$ (3,284)	\$ 736,849

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

Note 4. General Property, Plant, and Equipment, Net

DISA WCF general Property, Plant, and Equipment (PP&E) comprises telecommunications and computing services with related equipment, software, construction-in-progress, and assets under capital lease with a net book value (NBV) of \$1 billion.

The DISA WCF PP&E consists of telecommunications equipment, computer equipment, computer software, assets under capital lease, construction in progress, and leasehold improvements whereby the acquisition cost falls within prescribed thresholds and the estimated useful life is two or more years. The DISA WCF PP&E capitalization threshold is \$250 thousand for asset acquisitions and modifications/improvements placed into service after Sept. 30, 2013. PP&E assets acquired prior to Oct. 1, 2013, were capitalized at prior threshold levels (\$100 thousand for equipment and \$250 thousand for real property). PP&E with an acquisition cost of less than the capitalization threshold is expensed when purchased. Property and equipment meeting the capitalization threshold is depreciated using the straight-line method over the initial or remaining useful life as appropriate, which can range from two to 45 years.

The DISA WCF capitalizes improvements to existing General PP&E assets when the improvements equal or exceed the capitalization threshold and extend the useful life or increase the size, efficiency, or capacity of the asset. Leasehold improvements are amortized over the lesser of their useful life, generally five years, or the unexpired lease term.

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 DISA WCF's property and equipment, and all values are based on acquisition cost.

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

Figure 27-General Property, Plant, and Equipment, Net

(thousands)		
DISA WCF	CY	PY
General PP&E, Net beginning of year	\$ 908,288	\$ 890,603
Capitalized Acquisitions	156,961	142,786
Dispositions	(6,223)	(13,789)
Transfers in/(out) without reimbursement	198,907	115,397
Depreciation Expense	(242,360)	(226,710)
Balance at end of year	\$1,015,573	\$908,287

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 28-Major General PP&E Asset Classes

(thousands)					
DISA WCF 2022 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
Leasehold Improvements	S/L	Lease term	\$ 12,018	\$ (5,987)	\$ 6,031
Software	S/L	2-5 or 10	228,971	(152,096)	76,875
General Equipment	S/L	Various*	2,511,890	(1,651,940)	859,950
Assets Under Capital Lease	S/L	Lease term	316,863	(261,502)	55,361
Construction-in-Progress	N/A	N/A	17,355	N/A	17,355
Total General PP&E			\$ 3,087,097	\$ (2,071,525)	\$ 1,015,572

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

S/L= Straight Line N/A= Not Applicable

*TSEAS uses 5 years for depreciation and CS uses 3 years for most depreciation, unless otherwise specified.

Note 5. Liabilities Not Covered by Budgetary Resources

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

Intragovernmental liabilities-other comprise the DISA WCF's unfunded FECA liability in the amount of \$948 thousand. These liabilities will be funded in future periods.

Other than intragovernmental liabilities-federal employee benefits payable consist of various employee actuarial liabilities not due and payable during the current fiscal year. As of Sept. 30, 2022, DISA WCF's liabilities consist of actuarial FECA liability for workers' compensation benefits in the amount of \$4.1 million. These liabilities will be funded in future periods.

Figure 29-Liabilities Not Covered by Budgetary Resources

(thousands)		
DISA WCF	<u>2022</u>	<u>2021</u>
Intragovernmental Liabilities		
Other	\$ 948	\$ 1,009
Total Intragovernmental Liabilities	<u>948</u>	<u>1,009</u>
Other than Intragovernmental Liabilities		
Federal employee benefits payable	4,056	4,664
Total Other than Intragovernmental Liabilities	<u>4,056</u>	<u>4,664</u>
Total Liabilities Not Covered by Budgetary Resources	5,004	5,673
Total Liabilities Covered by Budgetary Resources	980,950	1,038,149
Total Liabilities	<u><u>\$ 985,954</u></u>	<u><u>\$ 1,043,822</u></u>

Note 6. Federal Employee Benefits Payable

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 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-M) 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 30- Compensation COLAs and CPI-Ms

CBY	COLA	CPI-M
2022	N/A	N/A
2023	3.37%	3.13%
2024	3.97%	3.62%
2025	4.10%	3.55%
2026	4.16%	3.84%
2027 and thereafter	3.91%	4.20%

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 2022 and FY 2021, respectively. Interest rate assumptions utilized for FY 2022 discounting were as follows:

Discount Rates

For wage benefits:

2.119 percent in Year 1 and years thereafter.

For medical benefits:

1.973 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 and 2022, respectively.

Expense Components

For FY 2022, the only expense component pertaining to other actuarial benefits for DISA WCF is the FECA expense. The Department of Labor (DOL) provides the expense data to DISA. The staffing ratio data from DISA headquarters determines the allocation of the expense to DISA WCF.

DOL provided an estimate for DISA's future workers' compensation benefits of \$7.8 million in total, of which \$4.1 million was distributed to 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. FECA liability, which falls under other actuarial benefits, decreased \$607.2 thousand due to a decrease in COLA and CPI-M inflation factors that in turn increased the actuarial liability estimate provided by DOL (<http://www.dol.gov/ocfo/publications.html>).

Figure 31-Federal Employee and Veteran Benefits Payable

(thousands)			
DISA WCF 2022	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
Other Benefits			
FECA	\$ 4,056	\$ -	\$ 4,056
Other	319	(319)	-
Total Other Benefits	4,375	(319)	4,056
Federal Employee Benefits Payable	4,375	(319)	4,056
Other benefit-related payables included in Intragovernmental Other Liabilities	2,746	(1,798)	948
Total Federal Employee Benefits Payable	\$ 7,121	\$ (2,117)	\$ 5,004
DISA WCF 2021	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
Other Benefits			
FECA	\$ 4,664	\$ -	\$ 4,664
Other	1,347	(1,347)	-
Total Other Benefits	6,011	(1,347)	4,664
Federal Employee Benefits Payable	6,011	(1,347)	4,664
Other benefit-related payables included in Intragovernmental Other Liabilities	5,531	(4,522)	1,009
Total Federal Employee Benefits Payable	\$ 11,542	\$ (5,869)	\$ 5,673

Note 7. Other Liabilities

Intragovernmental

Advances from others: \$257 thousand. This represents 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: \$45.8 million. DISA WCF reports the unpaid portion of accrued funded civilian payroll and employees' 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: \$59 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 Office of Personnel Management (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 32-Other Liabilities

(thousands)			
DISA WCF 2022	Current Liability	Non-Current Liability	Total
Intragovernmental			
Liabilities for Non-entity Assets	\$ -	\$ -	\$ -
Other Liabilities	-	-	-
Subtotal	-	-	-
Other Liabilities	2,294	452	2,746
Total Intragovernmental	2,294	452	2,746
Other than Intragovernmental			
Accrued Funded Payroll and Benefits	45,766	-	45,766
Total Other than Intragovernmental	45,766	-	45,766
	\$ 48,060	\$ 452	\$ 48,512
Total Other Liabilities	\$ -	\$ -	\$ -

DISA WCF 2021	Current Liability	Non-Current Liability	Total
Intragovernmental			
Liabilities for Non-entity Assets	\$ -	\$ -	\$ -
Other Liabilities	-	-	-
Subtotal	-	-	-
Other Liabilities	4,963	568	5,531
Total Intragovernmental	4,963	568	5,531
Other than Intragovernmental			
Accrued Funded Payroll and Benefits	57,534	-	57,534
Total Other than Intragovernmental	57,534	-	57,534
Total Other Liabilities	\$ 62,497	\$ 568	\$ 63,065

Note 8. Leases

Figure 33-Entity as Lessee - Assets Under Capital Lease (Table 16A)

(thousands)			
DISA WCF	2022	2021	
Equipment	\$ 316,863	\$ 363,716	
Accumulated Amortization	(261,502)	(300,122)	
Total Capital Lease	\$ 55,361	\$ 63,594	

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

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

DISA WCF has operating leases for land, buildings, and equipment. Future lease payments due as of Sept. 30, 2022, for non-cancelable operating leases were as follows:

Figure 34-Future Payments Due for Non-Cancelable Operating Leases (Table 16D)

(thousands)			
DISA WCF 2022	Land & Buildings	Equipment	Total
Federal			
Fiscal Year 2023	\$ 787	\$ 136	\$ 923
Fiscal Year 2024	732	-	732
Fiscal Year 2025	756	-	756
Fiscal Year 2026	780	-	780
Fiscal Year 2027	804	-	804
After 5 years	266	-	266
Total Federal Future Lease Payments	4,125	136	4,261
Total Non-Federal Future Lease Payments	-	-	-
Total Future Lease Payments	\$ 4,125	\$ 136	\$ 4,261

*DISA WCF does not currently have any non-federal future payments due for non-cancelable operating leases.

Land and Building Leases

As of Sept. 30, 2022, DISA WCF operates in 18 locations, of which 16 sites are located on property (primarily military bases) where no rent is charged and only utilities are required. The one remaining site is located on commercial property and covered under a long-term real estate lease expiring in 2028. The General Services Administration acquires and manages commercial property leases on behalf of the federal government; therefore, this lease is considered federal. This lease generally requires 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. DISA WCF currently leases 127 photocopiers and 22 vehicles located across various sites. The photocopiers are leased for three years, while the vehicles are leased for one year with annual renewal options.

DISA WCF does not currently have any non-federal future payments due for non-cancelable operating leases.

Note 9. Commitments and Contingencies

DISA WCF may be a party in various administrative proceedings and legal actions related to claims for environmental damage, equal opportunity matters, and contractual bid protests. 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 2022 reporting.

Note 10. Suborganization Program Costs

The Statement of Net Cost (SNC) represents the net cost of programs and organizations 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 programs 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 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 fiscal year 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 support 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, are shown for each line of business. The costs incurred and revenue earned for DISA WCF programs that received and provided services to one another have been adjusted and are not reflected in the totals. DISA WCF's services are priced to recover the full cost of resources consumed to produce the service.

Figure 35-General Disclosures Related to the Statement of Net Cost

(thousands)			
DISA WCF	2022	2021	
Operations, Readiness & Support			
Gross Cost	\$ 7,899,437	\$ 8,383,736	
Less: Earned Revenue	(7,808,452)	(8,105,542)	
Net Program Costs	<u>90,985</u>	<u>278,194</u>	
Consolidated			
Gross Cost	7,899,437	8,383,736	
Less Earned Revenue	(7,808,452)	(8,105,542)	
Total Net Cost	<u>\$ 90,985</u>	<u>\$ 278,194</u>	

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 36-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 2022
Computing Services				
Gross Costs	\$ (15,823)	\$ 31,309	\$ -	\$ 15,486
Less earned revenues	7	(78,484)	-	(78,477)
Net Costs	(15,817)	(47,175)	-	(62,991)
TSEAS				
Gross Costs	7,681,192	247,492	-	7,928,683
Less earned revenues	(1,150)	(7,740,688)	-	(7,741,838)
Net Costs	7,680,042	(7,493,197)	-	186,845
Component Level				
Gross Costs	(170,813)	170,813	(44,733)	(44,733)
Less earned revenues	-	-	11,864	11,864
Net Costs	(170,813)	170,813	(32,869)	(32,869)
Net Cost of Operations				
Gross Costs	7,494,556	449,614	(44,733)	7,899,437
Less Total Revenues	(1,143)	(7,819,172)	11,864	(7,808,452)
Total Net Costs	\$ 7,493,413	\$ (7,369,559)	\$ (32,869)	\$ 90,985
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)	-	(936,610)
Less earned revenues	-	936,610	-	936,610
Net Costs	(196,500)	196,500	-	0
Net Cost of Operations				
Gross Costs	7,935,033	455,035	-	8,390,067
Less Total Revenues	(12,848)	(8,099,025)	-	(8,111,873)
Total Net Costs	\$ 7,922,185	\$ (7,643,990)	\$ -	\$ 278,194

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

Note 11. Exchange Revenues

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 fiscal year 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 12. Inter-Entity Costs

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 support the summary information presented in the SNC and disclose 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 they are 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 37-Inter-Entity Costs

(thousands)		
Gross Program Costs	2022	2021
Gross Costs	\$ 7,899,437	\$ 8,383,736
Less: Earned Revenue	(7,808,452)	(8,105,542)
Net Cost of Operations	90,985	278,194
Bandwidth Management	168,053	210,039
Enterprise Accounting and Financial Management	74,436	41,801
IBM Mainframe Processing	73,692	87,758
Enterprise Internal IT Support	50,913	-
Other Programs	7,532,342	8,044,139
Less: earned revenue	(7,808,452)	(8,105,542)
Net other program costs:	\$ 90,985	\$ 278,194

The accompanying notes are an integral part of these statements.

Goods and services are received from other federal entities at no cost or at a cost less than the full cost to the providing federal entity. Consistent with accounting standards, certain costs of the providing entity that are not fully reimbursed are recognized as imputed costs in the Statement of Net Cost and are offset by imputed revenue in the Statement of Changes in Net Position. Such imputed costs and revenues relate to business-type activities, employee benefits, and claims to be settled by the Treasury Judgment Fund. However, unreimbursed costs of goods and services other than those identified above are not included in our financial statements.

Note 13. Statement of Budgetary Resources

As a revolving fund, DISA WCF budgetary resources are normally derived from customer reimbursements rather than direct appropriations. As such, obligated and unobligated amounts are generally not subject to cancellation that would affect the time period in which funds may be used.

As of Sept. 30, 2022, DISA WCF incurred \$7.5 billion in obligations, all of which are reimbursable and none of which are exempt from apportionment.

The total unobligated balance available (Apportioned) as of Sept. 30, 2022, is \$107.8 million and represents the cumulative amount of budgetary authority that has been set aside to cover future obligations for the current period.

As disclosed in Note 1, DISA WCF's SBR does not include intra-entity transactions as they have been adjusted to meet DISA's WCF one fund budgetary reporting requirements.

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

As of Sept. 30, 2022, DISA WCF's net amount of budgetary resources obligated for undelivered orders is \$740.2 million.

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

The amount of obligations incurred by DISA WCF may not be directly compared with the amounts reported on the *Budget of the United States Government* because DISA WCF funding is received and reported as a component of the "Other Defense Funds" program. The "Other Defense Funds" is combined with the service components and other DOD elements and then compared with the *Budget of the United States Government* at the defense agency level.

Figure 38-Budgetary Resources Obligated for Undelivered Orders at the End of the Period

(thousands)		
DISA WCF	2022	2021
Intragovernmental		
Unpaid	\$ 28,765	\$ 14,050
Total Intragovernmental	28,765	14,050
Non-Federal		
Unpaid	711,146	881,136
Prepaid/Advanced	257	401
Total Non-Federal	711,403	881,537
Total Budgetary Resources Obligated for Undelivered Orders at the End of the Period	\$ 740,168	\$ 895,587

Note 14. Reconciliation of Net Cost to Net Outlays

The reconciliation of Net Cost to Net Outlays demonstrates the relationship between 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 (proprietary) 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 DISA WCF's operations and financial position, including information about costs arising from the consumption of assets and the incurrence of liabilities. DISA's budgetary accounting office reports on the management of resources and the use and receipt of cash by DISA WCF. Outlays are payments to liquidate an obligation, excluding the repayment to Treasury of debt principal.

Figure 39- Reconciliation of the Net Cost of Operations to Net Outlays

(thousands)			
DISA WCF 2022	Intragovernmental	With the Public	Total
Net Cost of Operations (SNC)	\$ (7,380,839)	\$ 7,471,823	\$ 90,983
Components of Net Cost Not Part of Net Outlays:			
Property, plant, and equipment, net changes	-	107,284	107,284
Increase/(decrease) in assets:			
Accounts and taxes receivable, net	(158,508)	(43)	(158,551)
Other assets	-	(144)	(144)
(Increase)/decrease in liabilities:			
Accounts Payable	(14,054)	55,648	41,594
Federal employee benefits payable	0	1,635	1,635
Other liabilities	2,928	11,716	14,644
Other financing sources:			
Imputed cost	(23,075)	-	(23,075)
Total Components of Net Cost That are Not Part of Net Outlays	(192,709)	176,096	(16,613)
Miscellaneous Reconciling Items			
Total Other Reconciling Items	(198,938)	-	(198,938)
Total Net Outlays	\$ (7,772,486)	\$ 7,647,919	\$ (124,567)
Agency Outlays, Net, Statement of Budgetary Resources			(124,565)
Unreconciled difference			\$ (2)

*Unreconciled difference is due to rounding.

Note 15. Reclassification of Financial Statement Line Items for Financial Report Compilation Process

The DISA WCF does not have funds from dedicated collections and did not receive any supplemental appropriations during FY 2022.

**Defense Information Systems Agency
Working Capital Fund
Required Supplementary Information
Fiscal Year 2022, Ending Sept. 30, 2022**

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 FY 2022 to report. This determination is made based on existing contracts in place for current funded maintenance. Regularly scheduled maintenance takes place resulting in no need for deferred maintenance. DISA guidance and procedures are in place that address preventative maintenance as well as scheduled and unscheduled incidents requiring maintenance. Review is made for facilities, hardware, and software for current funding to deter operational and security issues. There is no request for WCF funding for deferred maintenance; hardware programs are at risk if current maintenance is not in place and if there would be a lack of maintenance for software, posing a security threat in DISA environment. Based upon these overarching considerations, preventative maintenance takes place with current contracts to ensure operational and security capabilities. Since it is anticipated, due to the nature of the mission, required maintenance is not deferred; therefore, not ranked or prioritized among other activities. In addition, as of FY 2022, all real property has been transferred out of the DISA WCF.

For FY 2022, 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 fiscal year.

Defense Information Systems Agency
Working Capital Fund
As of Sept. 30, 2022
(thousands)

Figure 40-Combining Statement of Budgetary Resources

	CS	TSEAS	Intra-Entity Eliminations	FY 2022
Budgetary Resources (discretionary and mandatory):				
Unobligated balance from prior year budget authority, net	\$ 677,228	\$ (548,963)	\$ (29,759)	\$ 98,506
Contract Authority (discretionary and mandatory)	(300)	188,381	-	188,081
Spending Authority from offsetting collections	(54,676)	5,155,792	2,259,174	7,360,290
Total Budgetary Resources	<u>622,252</u>	<u>4,795,211</u>	<u>2,229,415</u>	<u>7,646,877</u>
Status of Budgetary Resources:				
New obligations and upward adjustments (total)	(164,459)	5,474,114	2,229,415	7,539,070
Unobligated balance, end of year:	786,711	(678,903)	-	107,808
Apportioned, unexpired accounts				
Unexpired unobligated balance, end of year	786,711	(678,903)	-	107,808
Unobligated balance, end of year (total)	<u>786,711</u>	<u>(678,903)</u>	<u>-</u>	<u>107,808</u>
Total Budgetary Resources	<u>622,252</u>	<u>4,795,211</u>	<u>2,229,415</u>	<u>7,646,878</u>
Outlays, net:				
Outlays, net (total) (discretionary and mandatory)	(123,452)	(1,112)	-	(124,565)
Agency Outlays, net (discretionary and mandatory)	<u>\$ (123,452)</u>	<u>\$ (1,112)</u>	<u>-</u>	<u>\$ (124,565)</u>

**Defense Information Systems Agency
Working Capital Fund
Other Information
Fiscal Year 2022, Ending Sept. 30, 2022**

Management Challenges



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

02-Nov-2022

MEMORANDUM FOR DIRECTOR (D)

SUBJECT: Top Management and Performance Challenges Facing the Defense Information Systems Agency (DISA) in Fiscal Year 2023

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 and performance 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 2023.

In developing this report, the DISA OIG considered several criteria, including items such as the impact on safety and cybersecurity, 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 working in a hybrid work 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 Management and Performance Challenges for Fiscal Year 2023 include:

- Meeting Data Management Challenges
- Managing Human Capital in a Hybrid Work Environment
- Cyber Supply Chain
- Current and Future Contracting Environment
- Mission Partner Payments

RYAN.STEPHEN.M
ICHAEL.
Digitally signed by
RYAN.STEPHEN.MICHAEL.1300
Date: 2023.10.19 12:18:09 -04'00'

Stephen M. Ryan
Inspector General

Challenge 1

Meeting Data Management Challenges

Data management is the practice of collecting, keeping, and using data securely. 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.

The federal government, Department of Defense (DOD), and DISA, are under constant data-driven cyber attacks. For example, the Federal Bureau of Investigations (FBI), National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency (CISA) announced that Chinese state-sponsored hackers targeted and breached major telecommunications companies and network service providers and breached U.S. defense and technology firms. The hackers obtained passwords to gain access to the organizations' systems and intercept sensitive communications.

To help address these challenges, DOD outlined data management goals in the 2020 DOD Data Strategy. Per the Strategy, DOD aims to protect data and evolve data into actionable information for decision makers.

DISA has the responsibility to help DOD modernize infrastructure and identify, protect, detect, respond, and recover from data threats. DISA recently established the Chief Data Officer (CDO) and created DISA data scientist positions. In 2022, the CDO published the DISA Data Strategy Implementation Plan (IPlan) to describe a modern approach to information architecture and data management, outline workstreams necessary to organize activities, define future activities, and identify next steps for the DISA organization. DISA also created DISA Data Community of Excellence forum to bridge business policies, cyber, and information technology. In 2023, the DISA Office of the Inspector General (OIG) plans to assess DISA's progress in meeting the 2020 DOD Data Strategy and the 2022 IPlan.

Challenge 2

Managing Human Capital in a Hybrid Work Environment

COVID-19 forced DISA to change the way it operates to accomplish its mission through telework, new technologies, and tools enhancing communication, collaboration, and coordination, both internally and with mission partners. With new telework and remote work policies, DISA has transitioned to a hybrid work environment with most employees having the option to work from home more frequently. Moving forward in the hybrid work environment, DISA leadership will be presented with many of the same challenges faced during maximum telework, including maintaining employee morale and productivity, recruiting, and retaining talent, facility, and workspace management, and acquiring the necessary and relevant technology and tools.

Employee morale and productivity in the hybrid environment will continue to be challenging. As the workforce evolves, there will be many employees who never meet in person, bringing forth challenges with team bonding and socializing across the agency. DISA leadership will need to monitor morale and productivity; consider office culture; and ensure the workforce has the tools needed for collaboration in the hybrid environment.

Recruiting talent continues to be a challenge. DISA implemented new telework and remote work policies, allowing leadership to broaden the hiring pool of candidates in various geographical regions to attract and retain high quality talent. However, leadership will have to balance the use of telework and remote work to ensure mission requirements are met while providing the flexibilities to recruit and retain a skilled cyber workforce.

Facility and workspace management decisions continue to be impacted by the need to protect employees' health and safety in the current hybrid environment. We recognize the human capital improvements DISA has made for onboarding new employees and social distancing measures for protecting the health and safety of employees. However, continuing improvements may require updates to DISA's footprint worldwide, facility needs, and additional changes to the physical workspaces, including configuration modifications, furniture, audio/visual, technological tools, etc., having a considerable impact on the budget.

Workforce 2025 is the agency's plan to shape an empowered workforce, inspire trust through high trust behaviors, develop leaders, encourage bold decision-making, enable collaboration, embrace technological advancement, and optimize the hybrid workforce and hybrid workplace. The agency must rapidly adapt to inevitable technological advances and mission portfolio adjustments to ensure DISA delivers relevant, cutting-edge capabilities so our warfighters gain and maintain an operational and competitive edge.

Challenge 3

Cyber Supply Chain

Strengthening and securing DISA's cyber supply chain is an important 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.

To support this mission, DISA relies on an international supply chain to provide software, hardware, and services. The cyber supply chain includes a complex array of manufacturers, suppliers, and contractors. Cyber supply chain risk is the possibility that supply chain threats and vulnerabilities may intentionally or unintentionally compromise Information Technology (IT) or Operational Technology (OT) products and services.

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 interconnected nature of 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, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances.

In 2022, the DISA Office of the Inspector General (OIG) initiated an evaluation to assess DISA's Cybersecurity Supply Chain Risk Management program. The OIG is focusing on mapping the processes and stakeholders, as well as comparing the program to DOD, DISA, and industry requirements and best practices.

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 and ability to hire and retain talent, causing the inability to sufficiently and effectively meet DOD and other federal agency mission needs. DISA's Procurement Services Directorate (PSD)/Defense Information Technology Contracting Organization (DITCO) provides efficient and compliant procurement services for Information Technology, Cyber, and Telecommunication services that support national defense partners through timely, quality, and ethical contracting. PSD has turned away mission partner requests in the past year, resulting in lost revenue, due to PSD's mission requirements, increasing workload, and hiring 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, incomplete and unactionable procurement packages, unfunded requirement delays, and contract scope issues. Other challenges in contracting faced by PSD and mission partners are increased by the Office of Management and Budget (OMB), Office of the Secretary of Defense (OSD), DOD, and DISA funding levels, increased contract documentation, and other indirect process requirements. PSD and the Office of the Chief Financial Officer continue to collaborate to implement process improvements to fulfill contract requirements in a timely manner and meet mission partner needs.

The DISA Office of Inspector General (OIG) reported concerns relating to contracting at DISA; specifically, contracts pertaining to mobility devices, government-furnished property, cyber safeguards of defense information clause, contractor workspace designations, Government Purchase Card oversight, timely contract closeout, and management of unliquidated obligations. Additionally, the OIG identified concerns relating to Contracting Officer Representatives (CORs) 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. Overall, in FY 2022, the DISA DWCF managed approximately 3,190 computing orders, 13,422 PDCs, and 1,135 Telecommunication Military Interdepartmental Purchase Requests. DISA General Fund managed approximately 1,400 reimbursable projects.

Delinquent accounts receivable (AR) can take a significant amount of time and resources to resolve. 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 and sends formal collection memos on a periodic basis to the mission partners. Finally, if a mission partner is not reimbursing DISA according to the support agreement for services previously ordered, the OCFO calls the mission partner CFO directly. The DOD FMR allows for elevation to the Under Secretary of Defense Comptroller, Program Budget and/or Treasury for further collection action if warranted.

One can speculate why mission partners are waiting on payment submission closer to fiscal year end, including: funding uncertainties, reduced budgets, changes to Reimbursable Agreements, and penalties not applied to customers with delinquent accounts. Additionally, the move to G-Invoicing in October 2022, will also impact the mission partner collection process. G-Invoicing was developed to efficiently manage Intragovernmental Buy/Sell transactions between two federal agencies from the creation of the General Terms and Conditions (GT&C) to the Intragovernmental Payment and Collection system payment notification.

Delaying payment increases DISA's risk of not collecting payment by fiscal year end, while also putting a strain on the DWCF's budgetary resources to fund other mission requirements. The total past due AR on Sept. 30, 2022, totaled \$1.2 million in DISA Computing and \$14.4M in Telecommunications DWCF orders. The total past due AR for the DISA General Funds on Sept. 30, 2022, totaled \$21.7 million.

In 2022, the DISA Office of the Inspector General (OIG) initiated an audit of DISA's Reimbursable Services Collections to determine whether DISA collects AR for reimbursable services in accordance with DOD and DISA guidance.

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 provides are 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. The 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 to prepare 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 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 41-Summary of Financial Statement Audit

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

Figure 42-Effectiveness of Internal Control over Financial Reporting (FMFIA§ 2)**Statement of Assurance:** Unmodified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Fund Balance with Treasury	5	-	-	-	-	5
Accounts Payable/Expense	5	-	-5	-	-	-
Accounts Receivable/Revenue	2	-	-2	-	-	-
Internal Controls	1	-	-1	-	-	-
Unmatched Transactions	1	-	-1	-	-	-
Financial Reporting	1	-	-1	-	-	-
Undelivered Orders	2	-	-2	-	-	-
Unfilled Customer Orders	1	-	-1	-	-	-
PPE	-	1	-	-	-	1
Total Material Weaknesses	18	1	-13	-	-	6

Figure 43-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	-	-	-	-	-	-

Figure 44- 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	6	-	-6	-	-	-
Total non-conformance	6	-	-6	-	-	-

Figure 45-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, DFAS, as DISA's accounting service provider, performs overpayment recapture functions on behalf of DISA. DFAS includes DISA transactions in its sampling populations for improper payment testing of civilian payroll and travel. There have been no issues arising to merit an anticipated negative impact regarding payment integrity and improper payment recovery in FY 2022.

**DOD Office of Inspector General (OIG)
Audit Report Transmittal Letter**



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

December 15, 2022

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 2022 and FY 2021
(Project No. D2022-D000FL-0054.000, Report No. DODIG-2023-039)

We contracted with the independent public accounting firm of Kearney & Company, P.C. (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, 2022, and 2021. 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 the 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 2022, Volume 1, Volume 2 (Updated, June 2022), and Volume 3 (Updated, June 2022). 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, 2022, and 2021, 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 two material weaknesses related to the DISA Working Capital Fund's internal controls over financial reporting.*

Specifically, Kearney & Company concluded that DISA did not implement adequate controls to:

- reconcile and accurately report Fund Balance with Treasury; or
- record property, plant, and equipment activations, transfers, and disposals in a timely manner.

Kearney & Company's additional report, "Independent Auditor's Report on Compliance With Laws, Regulations, Contracts, and Grant Agreements," discusses one instance of noncompliance with provisions of applicable laws and regulations, contracts, and grant agreements. Specifically, Kearney & Company concluded that DISA did not comply with the Federal Managers' Financial Integrity 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 2022 and FY 2021 Financial Statements and related notes. Furthermore, we do not express conclusions on the effectiveness of internal control over financial reporting, on whether the 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 15, 2022 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.

A handwritten signature in dark ink that reads "Lorin T. Venable". The script is cursive and fluid, with the first name "Lorin" and last name "Venable" clearly legible.

Lorin T. Venable, CPA

Assistant Inspector General for Audit
Financial Management and Reporting

Attachments:

As stated

Independent Auditor's Report

INDEPENDENT AUDITOR'S REPORT

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

Report on the Audit of the Financial Statements

Opinion

We have audited the Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency (DISA), which comprise the Balance Sheets as of September 30, 2022 and 2021, the related Statements of Net Cost and Changes in Net Position, and the 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.

In our opinion, the accompanying financial statements present fairly, in all material respects, the financial position of DISA WCF as of September 30, 2022 and 2021 and its net cost of operations, 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.

Basis for Opinion

We conducted our audits in accordance with auditing standards generally accepted in the United States of America (GAAS); 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. 22-01, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards are further described in the ***Auditor's Responsibilities for the Audit of the Financial Statements*** section of our report. We are required to be independent of DISA WCF and to meet our other ethical responsibilities in accordance with the relevant ethical requirements relating to our audits. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Responsibilities of Management for the Financial Statements

Management is responsible for: 1) the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America; 2) the preparation, measurement, and presentation of Required Supplementary Information (RSI) in accordance with U.S. generally accepted accounting principles; 3) the preparation and presentation of Other Information included in DISA WCF's Agency Financial Report (AFR), as well as ensuring the consistency of that information with the audited financial statements and the RSI; and 4) 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.

In preparing the financial statements, management is required to evaluate whether there are conditions or events, considered in the aggregate, that raise substantial doubt about DISA WCF's ability to continue as a going concern for 12 months beyond the financial statement date.

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements, as a whole, are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and, therefore, is not a guarantee that an audit conducted in accordance with *Government Auditing Standards* will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

In performing an audit in accordance with *Government Auditing Standards*, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit
- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements
- Obtain an understanding of internal control relevant to the audit 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 DISA WCF's internal control. Accordingly, no such opinion is expressed
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements
- Conclude whether, in our judgment, there are conditions or events, considered in the aggregate, that raise substantial doubt about DISA WCF's ability to continue as a going concern for a reasonable period of time.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control-related matters that we identified during the audit.

Required Supplementary Information

Accounting principles generally accepted in the United States of America require that the RSI be presented to supplement the financial statements. Such information is the responsibility of management and, although not a part of the basic financial statements, is required by OMB and the Federal Accounting Standards Advisory Board (FASAB), who consider it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the RSI 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 basic financial statements, and other knowledge we obtained during our audits of the basic financial statements. We do 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.

Other Information

Management is responsible for the Other Information included in the AFR. The Other Information comprises the Summary of Financial Statement Audit and Manager Assurances, Management Challenges, and Payment Integrity sections, as named within the AFR, but does not include the financial statements and our auditor's report thereon. Our opinion on the financial statements does not cover the Other Information, and we do not express an opinion or any form of assurance thereon.

In connection with our audits of the financial statements, our responsibility is to read the Other Information and consider whether a material inconsistency exists between the Other Information and the financial statements or the Other Information otherwise appears to be materially misstated. If, based on the work performed, we conclude that an uncorrected material misstatement of the Other Information exists, we are required to describe it in our report.

Other Reporting Required by *Government Auditing Standards*

In accordance with *Government Auditing Standards* and OMB Bulletin No. 22-01, we have also issued reports, dated December 15, 2022, on our consideration of DISA WCF's internal control over financial reporting and on our tests of DISA WCF's compliance with provisions of applicable laws, regulations, contracts, and grant agreements, as well as other matters for the year ended September 30, 2022. 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. 22-01 and should be considered in assessing the results of our audits.

A handwritten signature in blue ink that reads "Kearney & Company". The signature is written in a cursive, flowing style.

Alexandria, Virginia
December 15, 2022

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

To the Director, Defense Information Systems Agency, and Inspector General of the Department of 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. 22-01, *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, 2022, and the related notes to the financial statements, which collectively comprise DISA WCF's basic financial statements, and we have issued our report thereon dated December 15, 2022.

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered DISA WCF's internal control over financial reporting (internal control) as a basis for designing 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 DISA WCF's internal control. Accordingly, we do not express an opinion on the effectiveness of DISA WCF's internal control. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 22-01. We did not 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 accompanying **Schedule of Findings**, we identified 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.



A *significant deficiency* is a deficiency, or combination of deficiencies, in internal control that is less 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 we will report to DISA WCF's management in a separate letter.

DISA WCF's Response to Findings

Government Auditing Standards requires the auditor to perform limited procedures on DISA WCF's response to the findings identified in our audit and described in the accompanying Agency Financial Report (AFR). DISA WCF concurred with the findings identified in our engagement. DISA WCF's response was not subjected to the other auditing procedures applied in the audit of the financial statements; accordingly, we express no opinion on the response.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and the results of that testing, and not to provide an opinion on the effectiveness of 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. 22-01 in considering the entity's internal control. Accordingly, this communication is not suitable for any other purpose.

A handwritten signature in blue ink that reads "Kearney & Company". The signature is stylized and cursive.

Alexandria, Virginia
December 15, 2022

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 Schedule of Findings have been formulated based on our determination of how individual control deficiencies, in aggregate, affect internal control over financial reporting. *Exhibit 1* presents the material 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. Property, Plant, and Equipment	A. Untimely Asset Disposal B. Untimely Asset Activation and Untimely Asset Transfers

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's service organization manages, reports, and accounts for Fund Balance with 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 DISA's 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 the last four digits of the fund account symbol identifies these funds. These clearing accounts are to be 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. DoD 7000.14-R, Financial Management Regulation (FMR), Volume 4, Chapter 2, Section 8.3, *Treasury Reconciliation Requirements* (020803), revised April 2020, states that differences recorded in Treasury Budget Clearing Accounts (suspense accounts) are reconciled monthly, as instructed in the Treasury Financial Manual (TFM), Volume I, Part 2, Chapter 5100, and moved to the appropriate Line of Accounting (LOA) within 60 business days from the date of transaction.

DISA suspense transactions, if any, are included and accounted for in Treasury Index (TI)-97 Other Defense Organizations (ODO), Department of the Navy (TI-17), Department of the Air Force (TI-57), and 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 contain DISA collections and disbursements that should be recognized in the DISA accounting records. While DISA's 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 or fiscal year (FY)-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 continue to contain a high volume of collections and disbursements which require manual research and resolution. DISA and its service organization have not designed and implemented a methodology to determine the financial reporting impact of DoD suspense account balances to DISA's financial statements for financial reporting in a timely manner sufficient for quarterly and annual financial reporting timelines.

Effect: DISA cannot identify and 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 Balance Sheet and other financial statement line items, as applicable.

Recommendations: Kearney & Company, P.C. (Kearney) recommends that DISA implement internal 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 DISA's service organization with necessary supporting documentation for corrections, if needed.
3. Consider any limitations to DISA's 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.

In addition, Kearney recommends that DISA coordinate with its service organization to perform the following:

1. 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 and made available for year-end financial reporting purposes.
2. Continue to monitor and track the resolution of suspense activity cleared to DISA to enable DISA to perform root cause analysis.
3. Continue to develop effective system and process controls to ensure that disbursements and collections are processed with valid TI, Treasury Account Symbol (TAS), and FY inputs.
4. 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 Processes

Background: DISA's service organization provides daily Non-Treasury Disbursing Office (NTDO) disbursing services under various Agency Location Codes (ALC), often referred to 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 reporting ALC 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 reporting any 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 Central Accounting Reporting System (CARS). The SoD report identifies discrepancies between the collections and disbursements reported to Treasury and what was actually processed for 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 and resolve DIT, IPAC, and Check Issued differences monthly. DISA's service organization has three 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 sufficient internal 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 or FY-end in a timely manner to perform sufficient analysis for financial reporting.

Cause: DISA's service organization's process to create the SoD Universe of Transactions (UoT) is a time-intensive and manual process that requires the consolidation of multiple files from various sources and subsequent manual research to identify the owners of the transactions. As such, the UoTs 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 and implemented a methodology to determine the financial reporting impact of the SoD balances to DISA's financial statements in a timely manner sufficient for quarterly and annual financial reporting timelines. While DISA's service organization has continued efforts to identify root causes by DSSN to reduce SoD balances and clear transactions to DoD entities timely, shared ALCs and lack of LOA information continue to make it difficult to resolve differences timely.

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

Recommendations: Kearney recommends that DISA implement internal 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. Assist DISA's service organization by providing supporting information to clear transactions timely.
2. Continue working with Treasury, the Office of the Secretary of Defense (OSD), DISA's service organization, and other parties to transition away from using monthly NTDO reporting ALCs to daily TDO reporting ALCs.
3. Consider any limitations to DISA's 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 DISA's 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.

In addition, Kearney recommends that DISA coordinate with its service organization to perform the following:

1. 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 and made available for year-end financial reporting purposes.
2. Continue to research and resolve SoD transactions in a timely manner.
3. Continue to assess and identify ALCs that primarily report collection and disbursement activity to Treasury on behalf of DISA.
4. 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.
5. Continue to schedule recurring meetings with DISA 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 TI-97 ODOs' disbursements and collections that have posted to 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 (T-SQL) programmed system developed by its 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 Information System (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, detect, and correct 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 its 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 data imported into DRRT back to original source systems. Additionally, DISA's service organization does 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 and implement effective FBWT reconciliation controls to ensure that accurate, complete, and properly supported financial data is included within the DRRT reconciliation. While DISA has made improvements from FY 2021, it 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, FBWT may 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:

1. Develop and implement procedures for effective communication with its service organization's management throughout the DRRT reconciliation process to ensure there

is DISA management review and approval of the data being attributed to DISA from DRRT.

2. Develop and implement effective controls to ensure the validation and/or review of the data received by its service organization, produced by DRRT, before it is recorded into DISA's GL system.
3. 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.
4. 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.

In addition, Kearney recommends that DISA coordinate with its service organization to perform the following:

1. 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.
2. Develop and implement effective procedures for its service organization 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. Property, Plant, and Equipment (*New Condition*)

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

- A. Untimely Asset Disposal
- B. Untimely Asset Activation and Untimely Asset Transfers

A. Untimely Asset Disposal

Background: The September 30, 2021 DISA WCF General Property, Plant, and Equipment (PP&E) is composed of leasehold improvements, equipment, software, assets under capital lease, and Construction-in-Progress (CIP) with a net book value (NBV) of \$908.3 million. DISA utilizes the Defense Property Accountability System (DPAS) as its property management system, which provides property financial reporting information.

DISA WCF categorizes leases as capital or operating based on the capital lease criteria defined by FASAB's Statements of Federal Financial Accounting Standards (SFFAS) No. 6, *Accounting for Property, Plant, and Equipment*. DISA's inventory of capital leases includes assets relating to its exclusive use of certain transoceanic cables in support of network communications as part

of the optical transport network. DISA is responsible for establishing controls to record asset disposals timely and accurately in DPAS.

Condition: DISA did not identify or remove five assets, out of a sample of seven, from its Balance Sheet that are no longer considered capital lease assets under new lease terms, totaling an acquisition value of \$30.5 million. Of the five exceptions, four of the assets should have been removed in FY 2017 and one should have been removed in FY 2021.

Cause: DISA did not have processes or internal controls to ensure that new lease terms agreed to with vendors were reviewed timely to make a capital vs. operating lease determination. DISA management only confirmed that the assets were still in use based on the existence of the circuits, but did not discover that the new contractual terms no longer met the criteria to be capitalized.

Effect: The assets had been fully depreciated in prior years so they did not have a net impact on DISA's Balance Sheet. However, the untimely asset disposal resulted in an overstatement of \$30.5 million acquisition and accumulated depreciation value on Footnote 10 of the September 30, 2021 financial statements. In addition, the lack of an effectively designed control increases the risk that a misstatement of a more material amount could occur and not be prevented, or detected and corrected, in a timely manner.

Recommendation: Kearney recommends that DISA implement an effective control and process to monitor agreements agreed to with vendors to perform a timely assessment of capital vs. operating leases for financial reporting purposes.

B. Untimely Asset Activation and Untimely Asset Transfers

Background: The September 30, 2021 DISA WCF General PP&E was composed of leasehold improvements, equipment, software, assets under capital lease, and CIP with NBV of \$908.3 million. DISA utilizes DPAS as its property management system, which provides property financial reporting information.

Starting in FY 2019, assets purchased using General Fund (GF) appropriations that will be utilized for the WCF are reported as CIP (United States Standard General Ledger [USSGL] 172000) on the GF until deployed from a DISA storage warehouse. When an asset is purchased by the GF and received from the storage warehouse as CIP, the date of shipment from the storage warehouse is used as the activation date for depreciation. When assets are a direct shipment to a facility, the DISA Capital Asset Management (CAM) Team receives e-mails from the site locations with the contract number and packing list, which the DISA CAM Team reviews to determine if the purchase includes capital assets.

In FY 2020, DISA implemented controls to identify equipment and labor costs received but not recorded in DPAS at FY-end. For direct shipments to DISA facilities, the receiving location notifies the DISA CAM Team via e-mail. The DISA CAM Team then identifies equipment received or disposed of and not recorded in DPAS at FY-end due to monthly "down-time" and

creates a JV to account for the costs. DISA is responsible for establishing controls to record assets timely and accurately in DPAS.

Condition: DISA management did not identify activated assets or transfer the assets from the GF to the WCF in a timely manner. The following errors were noted in DISA's PP&E account:

- DISA did not transfer Equipment with NBV of \$7.1 million and Software with NBV of \$10.5 million from the GF to the WCF and in the correct FY
- DISA did not record Equipment Ancillary costs with an acquisition cost of \$634 thousand in the correct FY
- DISA did not record assets with an activation date from FY 2021 in DPAS until FY 2022. These assets were composed of Equipment with NBV of \$1.6 million and Software with NBV of \$3.9 million
- DISA did not identify certain capitalized costs, referred to as equipment ancillary costs, of \$11.6 million until FY 2022 that should have been transferred to the WCF prior to September 30, 2021
- DISA processed a JV late in FY 2022 to transfer equipment with NBV of \$32.8 million from the GF to the WCF which should have been transferred in FY 2021. Additionally, DISA officials did not communicate this JV correction to the auditor timely.

Cause: The untimely asset activation and transfers generally resulted from inconsistent or ineffective communications between program officials responsible for the assets and the DISA officials who are responsible for property accounting. Many of the noted testing exceptions related to a new program (i.e., 4ENO Program). Specifically, DISA did not transfer assets timely from the GF to the WCF from the 4ENO Program because it was incorrectly identified as a program for the GF rather than the WCF. For the assets recorded through the year-end JV, the DISA CAM Team was not timely informed that the equipment was installed onsite by the vendor, as opposed to delivery to the CACI warehouse. Additionally, due to DISA's decentralized environment with equipment in locations world-wide, DISA personnel do not always provide documentation to the DISA CAM Team timely or possess a consistent understanding of property accounting requirements.

Effect: The untimely asset activation and transfers resulted in an understatement of approximately \$68 million NBV on the PP&E line of the Balance Sheet and the General Equipment cost on Footnote 9 of the September 30, 2021 financial statements. The untimely asset activation also resulted in an understatement of approximately \$3.4 million of depreciation on the Gross Costs line of the Statement of Net Costs, excluding the equipment ancillary assets due to the nature of the assets. The lack of an effectively designed control increases the risk that a material misstatement could occur and not be prevented, or detected and corrected, in a timely manner.

Recommendations: Kearney recommends that DISA perform the following:

1. Further develop an effective control and process to monitor assets for timely activation and ensure they are recorded in the financial statements in a timely manner by JV if received after the DPAS shutdown period.
2. Develop and implement a process to monitor CIP accounts on the GF to ensure timely transfers and review inventory reports from the DISA warehouse to monitor asset shipments.
3. Implement an effective control and process to notify the CAM Team when shipments arrive or depart site locations, in addition to enhanced coordination with Property Custodians on asset shipments.
4. Develop and implement a review process to ensure all new programs are designated to the correct Fund to ensure that DISA accurately records assets to the correct Fund's financial statements.
5. Conduct annual PP&E inventory to ensure assets noted on the inventory are identified in the current FY's financial statements.
6. Increase communication between the DISA CAM Team, DISA Financial Management Team, and DISA's main program officials who are responsible for significant property inventories. This may include property management and property accounting training programs for DISA's program officials.

* * * * *

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 control over 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	<ul style="list-style-type: none"> A. Lack of Documentation of Defense Information Systems Agency Management's Assessment Related to its Reporting Entity per Statement of Federal Financial Accounting Standards Requirements B. Agency Financial Report Omissions, Errors, and Noncompliance C. Inaccurate Expired Commitment Adjustment
II. Information Technology	<ul style="list-style-type: none"> A. Financial Accounting and Budget System Application Audit Logging and Monitoring B. Defense Information Systems Agency Risk Management Framework C. Inconsistent Budget and Execution Reporting Tool Change Management Process D. Incomplete Financial Accounting and Budget System Application Access Request Documentation E. Financial Accounting and Budget System Change Management Process F. Financial Accounting Management Information System – Working Capital Fund Removal of Inactive and Separated Users G. Budget and Execution Reporting Tool Database Audit Logging and Monitoring H. Financial Accounting Management Information System – Working Capital Fund Database Audit Logging and Monitoring I. Incomplete Complementary User Entity Controls Implementation

I. Financial Reporting (*Repeat Condition*)

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

- A. Lack of Documentation of Defense Information Systems Agency Management's Assessment Related to its Reporting Entity per Statement of Federal Financial Accounting Standards Requirements
- B. Agency Financial Report Omissions, Errors, and Noncompliance
- C. Inaccurate Expired Commitment Adjustment

A. Lack of Documentation of Defense Information Systems Agency Management's Assessment Related to its Reporting Entity per Statement of Federal Financial Accounting Standards Requirements

Background: FASAB's 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. 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.

In response to prior-year findings, DISA implemented a procedure to review the SFFAS guidance related to No. 47 and document any updates via a checklist and assessment. DISA did not have procedures to perform a documented review of its reporting entity in accordance with SFFAS No. 47.

Condition: Although DISA implemented procedures to assess the requirements of SFFAS No. 47, the procedures were not performed in a timely manner. Additionally, the procedures did not include steps to confirm the completeness of the reporting entity, financial statements, or related disclosures in accordance with SFFAS No. 47.

Cause: DISA has not fully developed or implemented sufficient documented controls to ensure that it has complied with SFFAS No. 47. DISA has not developed procedures to periodically confirm the completeness of its reporting entity, such as analyzing its basic symbols and reporting limits within a separately documented management-approved assessment.

Effect: The lack of a comprehensive SFFAS No. 47 assessment increases the risk that DISA's financial statements may omit consolidation entities and/or disclosure entities, as required by the Standard. Further, the Government-wide GPFFR may be incomplete as a result of any missing consolidation or disclosure entities. In addition, if this assessment is performed late in the FY, DISA may lack sufficient time to properly adjust its financial statements and disclosures based on the conclusions of the assessment.

Recommendations: Kearney recommends that DISA perform the following:

1. Expand and document its procedures and controls relating to SFFAS No. 47 to include documented steps to validate the completeness of its reporting entity, such as an analysis of the appropriateness of its basic symbols and reporting limits.
2. Implement the expanded procedures and controls early in the FY, prior to preparing interim financial statements and note disclosures, to allow for sufficient time to process any adjustments resulting from the assessment.

B. Agency Financial Report Omissions, Errors, and Noncompliance

Background: DISA utilizes a service organization that is responsible for the agency's 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. Additionally, DISA is responsible for ensuring all quality control (QC) reviews occur and compliance updates are made prior to publication.

Condition: DISA WCF's Quarter (Q) 4 draft AFR contained errors, omissions, and inconsistencies not identified by DISA management. For example, there were errors related to financial statement/footnote balance cross-footing throughout the components of the AFR (e.g., Management's Discussion and Analysis [MD&A], principal financial statements, and footnotes and disclosures). The AFR also contained various editorial errors that were not detected and corrected throughout the QC review process. In addition, there were various missing and omitted OMB Circular A-136 components that were noted during reviews of the draft AFR, such as the following:

- Section II.1.1 – Missing statement providing reasonable assurance over the completeness and reliability of the financial data
- Section II.1.4.1 – Omitted the required tables and information within the *Other Information* section
- Section II.3.8.32 – No reconciliation was included within the submission, as required by OMB Circular A-136
- Section II.3.8.34 – Omitted the required disclosure on DISA WCF's related party activity.

Cause: Although it has implemented various remediation efforts and coordinated multiple draft AFR submissions for review prior to the noted deadlines, DISA does not yet have the necessary control environment and consistent QC processes to ensure the content of the AFR is complete,

accurate, and in compliance with OMB Circular A-136 requirements. Prior to its final AFR submission to the specific requesting parties (e.g., independent audit firms, Office of the Under Secretary of Defense [Comptroller] [OUSD(C)]), DISA relies on its service organization to prepare its AFR. The division of responsibilities between DISA and its service organization for ensuring the effectiveness of that review has not yet been sufficiently delineated as demonstrated by the discrepancies and errors identified and communicated to DISA during the audit.

Effect: DISA made various corrections and incorporated updates to the additional information included in its FY 2022 AFR prior to finalization in order to ensure the document complied with the appropriate OMB requirements. However, not all updates were made throughout the resubmitted AFR. As a result, 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 in future periods.

Recommendations: Kearney recommends that DISA perform the following:

1. Continue to review, implement, and document the processes and internal control environment relating to the accumulation and review of the data utilized to prepare the AFR and confirm that disclosures, supporting tables, reconciliations, and analytical information reported in the AFR are reasonable and accurate.
2. 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 the content presented.
 - b. Ensure all the information compiled into the AFR is reviewed at a sufficient level by DISA management to ensure accuracy, completeness, and compliance with requirements.
 - c. Document evidence of the detail review(s).
3. Develop and maintain appropriate timeframes of DISA management's, as well as DISA's service organization's, reviews and updates to ensure all AFR content, whether draft or final, is submitted by the noted deadlines from various parties.

C. Inaccurate Expired Commitment Adjustment

Background: USSGL Account 422100, *Unfilled Customer Orders (UCO) Without Advance*, represents 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 Military Interdepartmental Purchase Request (MIPR), contract, or sales order, to provide goods and/or services when a customer cash advance is not received. These orders provide obligational budgetary authority for reimbursable programs. Agencies should maintain policies and procedures to ensure that UCOs represent valid future billings and collections.

DISA WCF reported \$3.1 billion in UCOs on its September 30, 2022 trial 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.

DISA developed an annual control to identify all projects with open and expired commitments. Expired commitments no longer represent valid UCOs. At the end of the FY, projects with remaining balances are reviewed for expired commitments and reduced through a JV, if the de-obligation cannot be recorded prior to year-end, due to timing constraints. The adjustment is posted annually in FAMIS-WCF as a temporary JV and is reversed in the subsequent month. DISA creates an Executive Summary document for budgetary adjustments, which includes the background, analysis, and GL impacts of the adjustment and is reviewed by DISA management. Once the financial system opens in FY 2022, DISA can process the de-obligation. It is DISA management's responsibility to ensure that all adjustments recorded are appropriate.

Condition: The temporary JV recorded by DISA during FY 2021 to reduce its UCO balance for expired commitments did not reverse in the subsequent month and remained in FAMIS-WCF in FY 2022. DISA de-obligated the UCOs during FY 2022; therefore, the FY 2021 adjustment was no longer needed.

Cause: Although DISA management designed a process for all JVs to be reviewed, the reviewing official did not identify that the JV was inaccurately designated as a permanent JV, rather than a temporary JV. Therefore, DISA did not reverse the FY 2021 adjustment for UCOs with expired commitments in FY 2022, which caused an understatement to the Statement of Budgetary Resources (SBR) line 1890, *spending authority from offsetting collections*.

Effect: Ineffective controls to monitor JVs for accuracy increases the risk that DISA may adjust its financial statements and records inaccurately. As a result of this error, DISA understated its SBR line 1890, represented by UCOs in FY 2022 by \$21.5 million.

Recommendation: Kearney recommends that DISA consider additional steps to ensure that its internal controls are operating effectively. This may include additional procedures to monitor JVs for accuracy and training procedures for officials responsible for reviewing JVs.

II. Information Technology (*Repeat Condition*)

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

- A. Financial Accounting and Budget System Application Audit Logging and Monitoring
- B. Defense Information Systems Agency Risk Management Framework
- C. Inconsistent Budget and Execution Reporting Tool Change Management Process
- D. Incomplete Financial Accounting and Budget System Application Access Request Documentation
- E. Financial Accounting and Budget System Change Management Process
- F. Financial Accounting Management Information System – Working Capital Fund Removal of Inactive and Separated Users
- G. Budget and Execution Reporting Tool Database Audit Logging and Monitoring
- H. Financial Accounting Management Information System – Working Capital Fund Database Audit Logging and Monitoring
- I. 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 Force Base (AFB) are responsible for information system security, including logging and monitoring controls, for the Financial Accounting and Budget System (FABS). FABS manages and tracks the financial aspects (e.g., Accounts Payable [AP], vendor invoices, vouchers) associated with telecommunication circuits, equipment, and services leased from various carriers/vendors on behalf of the Government through Defense Working Capital Fund (DWCF)/Telecommunications Services and Enterprise Acquisition Services (TSEAS). FABS also supports customer billing, indicating monthly recurring charges, nonrecurring 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 for an 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 incorporate a review nor documentation detailing how personnel would complete such a review. For example, DISA did not finalize documentation detailing a process to perform a review, including the frequency of review, maintenance of review documentation, and documentation of actions taken as a result of the review.

Cause: As of April 2021, DISA personnel had developed a process to log all security authorization modifications to the FABS application; however, due to continued timing constraints and prioritization of additional high-importance projects, DISA was unable to implement a review of the logs to include actions taken on account modifications captured, as well as finalizing documentation surrounding 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, and return account privileges to the original state.

Recommendations: Kearney recommends that DISA perform the following:

1. Finalize documented 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. Defense Information Systems Agency Risk Management Framework

Background: DISA is a U.S. DoD Combat Support Agency that provides enterprise services, unified capabilities, and mobility options to support DoD worldwide operations. DISA meets the DoD's information technology (IT) needs through enterprise security architectures, smart computing options, and other leading-edge IT opportunities. Specifically, DISA delivers hundreds of IT support services and capabilities and has the capacity to host, support, engineer, test, and/or acquire IT services.

As described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision (Rev.) 2, *Risk Management Framework for Information Systems and Organizations*, the Risk Management Framework (RMF) provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels. The RMF also promotes near-real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle. Executing the RMF tasks links essential risk management processes at the system level to risk management processes at the organization level. In addition, it establishes responsibility and accountability for the controls implemented within an organization's information systems and inherited by those systems.

DISA utilizes Enterprise Mission Assurance Support (eMASS) to implement the RMF to its respective systems. eMASS is a web-based Government Off-the-Shelf (GOTS) solution that automates a broad range of services for comprehensive, fully integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of RMF for DoD IT Package Reports. eMASS utilizes organizationally defined values prescribed by the Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection For National Security Systems*. Specifically, CNSSI No. 1253 provides National Security System (NSS)-specific information on tailoring, developing, and applying overlays for the national security community and parameter values for NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, security controls that are applicable to all NSSs.

The CNSS collaborates with NIST to ensure NIST SP 800-37; NIST SP 800-53; and NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, address security and privacy safeguards to meet the requirements of NSSs to the extent possible and provide a common foundation for information security and privacy across the U.S. Federal Government. CNSSI No. 1253 is a companion document to the NIST publications relevant to the RMF Steps Categorize and Select (i.e., NIST SP 800-37; NIST SP 800-53; NIST SP 800-53B; NIST SP 800-60, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST SP 800-60, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*; and Federal Information Processing Standards [FIPS] Publication [PUB] 199, *Standards for Security Categorization of Federal Information and Information Systems*).

In September 2020, NIST published Rev. 5 of NIST SP 800-53. Per OMB Circular A-130, *Managing Information as a Strategic Resource*, organizations have a one-year grace period prior to finalizing their implementation of any updated requirements.

Condition: As of August 2022, DoD policy and CNSSI No. 1253 had not been aligned to NIST SP 800-53, Rev. 5 in the prescribed timeline set forth by OMB Circular A-130 (i.e., one-year implementation post-publication). As a result, DISA did not update its RMF documentation, processes, or procedures to reflect updated requirements presented within NIST SP 800-53, Rev. 5. Furthermore, DISA personnel did not revise their system-specific security documents, such as System Security Plans (SSP) or related documentation (e.g., Security Design Documents [SDD]) to reflect requirements detailed in NIST SP 800-53, Rev. 5.

Cause: As eMASS utilizes CNSSI No. 1253 parameter values for NIST SP 800-53 security controls, eMASS, the DoD, and, therefore, DISA, rely on the CNSS to update their CNSSI No. 1253 baselines prior to transitioning to NIST SP 800-53, Rev. 5 controls. Following updates to the CNSSI No. 1253 baselines, the DoD will begin a formal uplift to transition to the NIST SP 800-53, Rev. 5 requirements. As of August 2022, updates to the CNSSI No. 1253 baselines were still in progress.

Effect: The success of an entity's missions and business functions depends on protecting the confidentiality, integrity, and availability of information processed, stored, and transmitted by their respective systems. Without a fully implemented and effective RMF process, associated security control selection and implementation, or documentation supporting the design of those security controls, entities may be susceptible to threats against their operating environments, which could result in damage to an entity's operations, assets, individuals, or other entities.

Recommendations: Kearney recommends that DISA perform the following:

1. Coordinate with the DoD to remain up to date regarding updates to CNSSI No. 1253 baselines, as well as subsequent updates made to eMASS, to ensure timely implementation of DISA's RMF.
2. Implement the RMF and revise system-specific security documentation, including control selection and implementation, to reflect requirements detailed in NIST SP 800-53, Rev. 5.
3. Once implementation of NIST SP 800-53, Rev. 5 security controls has been finalized, conduct authorizations and continuous monitoring of their respective systems in accordance with NIST SP 800-53, Rev. 5 requirements.

C. Inconsistent Budget and Execution Reporting Tool Change Management Process

Background: The DISA Financial Management Liaison Office (FMLO), located in Pensacola, FL, is responsible for information system security and configuration Change Management (CM) for the Budget and Execution Reporting Tool (BERT). BERT is an online management information system used by the DISA Enterprise Services Directorate (ESD), Chief Financial Executive (CFE) and Accounting Integration and Financial Reporting Office (CFA3) to provide a standardized method for budget preparation, rate development, and execution of cost and revenue, to include reporting and querying capabilities.

According to NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, configuration change control is the documented process for managing and controlling changes to the configuration of an information system or its constituent configuration items. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control is applied to include changes to components of the information system, changes to the configuration settings for IT products, emergency/unscheduled changes, and changes to remediate flaws. Changes are controlled from the time the change is proposed to the testing and implementation of the change. Each step in the change process is clearly articulated, along with the responsibilities and authorities of the roles involved.

Condition: DISA personnel did not maintain a complete and accurate listing of changes implemented within the BERT production environment. In addition, DISA personnel did not update the Change Control Board (CCB) Standard Operating Procedures (SOP) for FMLO CCB to reflect updates made to their CCB members and CM repository.

Cause: Throughout FYs 2021 and 2022, DISA began development and implementation of the One Fund Program. The One Fund Program's purpose is to establish a single DISA WCF environment by consolidating the two existing WCF entities (i.e., Computing Services [CS] and TSEAS) into a single fund. As a result, DISA personnel sunset Serena Business Manager (SBM) and moved BERT's CM repository to SharePoint Online. Due to the move to SharePoint Online and One Fund transition, DISA personnel maintained a manual spreadsheet of changes; however, once BERT's SharePoint Online CM repository was implemented, DISA personnel did not maintain, nor update, the listing timely to include changes that affected the BERT production environment.

Effect: By failing to consistently maintain an up-to-date and accurate listing of BERT changes, DISA personnel may not be fully aware of changes made to the BERT application. Further, personnel may not be able to identify configurations that impact the security posture of the information system and organization.

Recommendations: Kearney recommends that DISA perform the following:

1. Update procedural documentation to reflect updates made to BERT CCB members, technology utilized, as well as any additional updates to BERT's CM processes.
2. Consistently implement BERT's documented CM processes to ensure DISA personnel maintain a complete and accurate listing of changes implemented within the BERT production environment.
3. Develop and implement QC review procedures to supplement the BERT configuration CM process. These QC reviews should ensure that all BERT changes follow a defined and controlled process, including maintaining appropriate supporting documentation from initial change request through implementation in the production environment.

D. Incomplete Financial Accounting and Budget System Application Access Request Documentation

Background: The DISA personnel located at FGGM and Defense Information Technology Contracting Office (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 DWCF/TSEAS. FABS also supports customer billing, indicating monthly recurring, non-recurring, and overhead charges.

DISA controls initial account access to the FABS application through the receipt of a completed and reviewed Department of Defense (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. External users must submit a DD Form 2875, *SAAR*, in addition to the User Account Access Checklist (internal SAAR form) through the Enterprise Security Posture System (ESPS)/System Access Management (SAM) solution implemented in November 2021. This request requires the prospective user to have completed security awareness training, provided required personal information, and included the approval signatures of the user’s supervisor and the user’s local security manager. The user’s supervisor then routes the completed SAAR forms to the System Administrator (SA) group to obtain final approval and processing from the FABS Data Owner. The SA group identifies the applicable Data Owner residing in DISA’s Office of Accounting Operations and Compliance (CFA) or DITCO – Scott Procurement Services Directorate (PL13). The Data Owner then conducts the final review of the DD-2875 and signs the form, indicating approval.

Once the Data Owner provides the final approval, the SAs create the new user’s account and contact the supervisor if further clarification is needed. Internal users follow the same process as the external users; however, they are only required to use the User Account Access Checklist in place of the SAAR through ESPS/SAM.

NIST SP 800-53, Rev. 5 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 management reviewed and approved the access permissions granted for seven out of 11 users (approximately 64%) who received access to the FABS application from October 1, 2021 through May 9, 2022. Specifically, DISA was unable to provide evidence of requested facility codes (e.g., permissions) or Data Owner approval for seven users.

Cause: In March 2022, DISA personnel updated their 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 effective QC 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, there is increased risk that users may receive inappropriate access to the FABS application.

Recommendation: Kearney recommends that DISA 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.

E. Financial Accounting and Budget System Change Management Process

Background: The DISA personnel located at FGGM and DITCO – Scott AFB are responsible for information system security and CM for the 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 DWCF/TSEAS. FABS also supports customer billing, indicating monthly recurring, non-recurring, and overhead charges.

According to NIST SP 800-128, configuration change control is the documented process for managing and controlling changes to the configuration of an information system or its constituent configuration items. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control is applied to include changes to components of the information system, changes to the configuration settings for IT products, emergency/unscheduled changes, and changes to remediate flaws. Changes are controlled from the time the change is proposed to the testing and implementation of the change. Each step in the change process is clearly articulated, along with the responsibilities and authorities of the roles involved.

In FY 2022, DISA personnel managing the FABS application transitioned the FABS configuration CM process from DoD Enterprise Services Portal Services (DEPS) to DoD SharePoint Online. DISA personnel utilize the DoD SharePoint Online to manage the FABS application configuration CM process from initial request through implementation of requested, approved changes to the application production environment. The FABS configuration CM process includes the involvement of a CCB, which is a designated governing body to set configuration management objectives and priorities and oversee configuration item (CI) development and deployment activities. Further, DISA personnel designed workflows illustrating the FABS Change Request (CR) processes. The Business Systems Division's (SD2) workflow requires CRs to flow through the Initiation Team and CCB for review. Subsequently, DISA personnel test and evaluate the CR before final deployment approval is granted.

Condition: DISA personnel did not ensure all FABS application changes followed a defined and controlled process in accordance with DISA's policies and procedures. Specifically, DISA did not consistently obtain and document required approvals throughout the process of developing, testing, and implementing two of five (40%) sampled FABS application changes that DISA implemented throughout FY 2022. Examples included documented testing occurring after DISA implemented a change and no documented CCB approval prior to implementing a change.

Cause: In April 2022, DISA personnel managing the FABS application transitioned their CR process from DEPS to DoD SharePoint Online. As a result, DISA personnel did not verify or ensure that the updated DoD SharePoint Online process and related FABS CR forms tracked and maintained all pertinent information and documentation related to requested FABS application changes. DISA personnel stated that they are in the process of updating the DoD SharePoint tool to ensure changes follow FABS configuration change processes, to include tracking and retention of documentation to support changes implemented into the FABS production environment.

Effect: By failing to ensure all FABS application changes follow a defined and controlled process with sufficient documentation to support all required phases of the configuration CM process, DISA personnel may not be fully aware if changes were appropriately developed, tested, and implemented. Further, implementing application changes prior to testing and approval increases the risk that vulnerabilities or unwanted functionalities may be unknowingly introduced within the application, which could affect the confidentiality, integrity, and availability of DISA's data processed in FABS.

Recommendations: Kearney recommends that DISA perform the following:

1. Update procedural documentation to reflect updates made to technologies utilized, as well as any additional updates made to FABS's CM processes and associated required support.
2. Ensure updates made to the FABS configuration CM tool include fields to track CRs from initial request to implementation into the production environment.
3. Consistently maintain documentation to support that configuration changes made to the FABS application align with updates made to the FABS configuration management tool.
4. Develop and implement QC review procedures to supplement the FABS configuration CM process. These QC reviews should ensure that all FABS changes follow a defined and controlled process, including maintaining appropriate supporting documentation from initial change request through implementation in the production environment.

F. Financial Accounting Management Information System – Working Capital Fund Removal of Inactive and Separated Users

Background: The DISA FMLO, located in Pensacola, FL, is responsible for information system security management and the removal of inactive and separated users for FAMIS-WCF.

FAMIS-WCF is a turn-key Financial Management System Software (FMSS) solution. The solution is based on Oracle eBusiness Suite (EBS) R12.2.9 to support the following application family of products: General Ledger, Accounts Receivable, Accounts Payable, Federal Administration, Project Costing, Project Billing, Project Contracts, Purchasing, and iProcurement. The resulting system implements Oracle Identity and Access Management (IAM) to interface with EBS to provide Common Access Card (CAC) authentication to EBS.

DISA personnel control account access removal for the FAMIS-WCF application. The SAs are responsible for ensuring that access to the FAMIS-WCF application is terminated upon departure of the employee. The SAs are notified via e-mail to deactivate the accounts, and accounts are to be systemically deactivated after 35 days of inactivity.

NIST SP 800-53, Rev. 5 informs individuals responsible for information systems that removing or disabling terminated or separated users' access in a timely manner at the application layer provides increased information security. Inappropriate user access/privileges increases the risk to the confidentiality, integrity, and availability of the systems and its data.

Condition: DISA personnel did not remove or disable users' access to the FAMIS-WCF application upon separation from DISA. Specifically, three FAMIS-WCF application users retained their access, ranging from 25 to 99 days past their date of separation. DISA did not remove the users' access until April 13, 2022.

Cause: DISA's process for removing or disabling FAMIS-WCF application access for users who separate from the agency requires SAs to manually remove accounts upon notification of the separation or the system to disable users' accounts after 35 days of inactivity. DISA personnel did not receive notification to remove the three users upon their departure, and the nightly automated process for disabling accounts after 35 days of inactivity malfunctioned, causing these users to retain access past their separation dates.

Effect: By failing to remove users' access in a timely manner, DISA increases the risk that users may have inappropriate access. Additionally, DISA does not have reasonable assurance that it would identify 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:

1. Enforce documented policies and procedures in DISA's *Risk Assessment for FAMIS-WCF* and the *FAMIS-WCF SSP*, as amended, regarding access control for the FAMIS-WCF application account deactivation process.
2. Develop and implement a QC process over the user removal process. The QC process should include procedures to ensure removal of FAMIS-WCF users' accounts after separation.

G. Budget and Execution Reporting Tool Database Audit Logging and Monitoring

Background: DISA FMLO, located in Pensacola, FL, is responsible for information system security, including review of audit logs for BERT. BERT is an online management information system used by the DISA ESD, CFE, and CFA3 to provide a standardized method for budget preparation, rate development, and execution of cost and revenue, to include reporting and querying capabilities.

According to NIST SP 800-92, *Guide to Computer Security Log Management*, routine log reviews and analyses are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, as well as for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems. In addition, organizations should establish policies and procedures for log management, prioritize log management appropriately, and provide proper support for all staff with log management responsibilities.

DISA utilizes SQL Server to log configuration changes made to the BERT database. DISA personnel have configured the BERT database to automatically generate alerts and weekly reports based on predefined criteria and then subsequently route those alerts to the BERT database administrator (DBA) and applicable personnel for analysis and review.

Condition: While DISA implemented a process to log and review configuration changes to the BERT database weekly, DISA personnel did not adhere to the required review timeframe of seven days following the generation of weekly audit log reports. Specifically, DISA personnel did not perform timely reviews for eight of the nine (approximately 89%) BERT database audit logs sampled for testing. In addition, additional oversight review was not indicated for five of nine (approximately 56%) database audit logs sampled for testing.

Cause: In FY 2020, DISA personnel successfully developed and implemented a process to log and review all configuration changes made to the BERT database. However, in FY 2022, DISA personnel were unable to perform reviews in a timely manner without additional oversight due to workload prioritization and personnel departures.

Effect: By not reviewing BERT database audit logs in a timely manner, DISA personnel may not be aware of potential issues that could affect the BERT database. Those issues may affect the integrity and availability of the BERT database, as well as the security baseline. Untimely audit log reviews may result in inappropriate or malicious actions going undetected for an extended period, which may hinder DISA's ability to initiate prompt corrective action. Additionally, by not including secondary oversight when an individual is reviewing data that they are responsible for on a day-to-day basis, DISA risks the possibility of BERT database log errors not being identified or misuse of data.

Recommendations: Kearney recommends that DISA perform the following:

1. Update BERT procedural documentation to provide instruction regarding backfilling positions when initial designated review personnel may be unable or unavailable to perform assigned BERT database log review responsibilities. DISA should ensure documentation includes information regarding secondary independent reviews to establish additional oversight to avoid users reviewing their own work.
2. Ensure review of BERT database logs are completed within prescribed timelines (i.e., seven days), as required by DoD-wide guidance, and retain evidence of the review of BERT database logs for third-party review.
3. Develop and implement a QC process over the BERT database logging and monitoring review process. The QC process should include procedures to ensure BERT database logs are reviewed within the prescribed timeline and that personnel are not the sole reviewers over processes for which they are responsible on a day-to-day basis.

H. Financial Accounting Management Information System – Working Capital Fund Database Audit Logging and Monitoring

Background: The DISA FMLO, located in Pensacola, FL, is responsible for information system security management and audit logging and monitoring for FAMIS-WCF.

As a turn-key FMSS solution, FAMIS-WCF, which is based on Oracle EBS R12.2.9, supports the following application family of products: General Ledger, Accounts Receivable, Accounts Payable, Federal Administration, Project Costing, Project Billing, Project Contracts, Purchasing, and iProcurement. The resulting system implements Oracle IAM to interface with EBS to provide CAC authentication to EBS.

According to NIST SP 800-92, routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred and for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems. In addition, organizations should establish policies and procedures for log management, prioritize log management appropriately, and provide proper support for all staff with log management responsibilities.

DISA utilizes Oracle to log configuration changes made to the FAMIS-WCF database. The FAMIS-WCF DBAs have configured the database to automatically initiate daily e-mail-generated reports based on predefined criteria for analysis and review. Subsequently, the DBAs route the e-mail-generated reports to the appropriate personnel (i.e., Information System Security Manager [ISSM]) for analysis and review.

Condition: While DISA implemented a process to log and review configuration changes to the FAMIS-WCF database daily, DISA personnel did not adhere to the required review timeframe of seven days following the generation of daily e-mail-generated audit log reports. Specifically,

DISA personnel did not perform timely reviews for two of the 37 (approximately 5%) FAMIS-WCF database audit logs sampled for testing. Further, DISA personnel did not perform reviews for three of the 37 (approximately 8%) FAMIS-WCF database audit logs sampled for testing.

Cause: DISA personnel implemented a process to log all configuration changes to the FAMIS-WCF database; however, in February 2022, DISA updated the FAMIS-WCF Oracle database. This update resulted in a temporary failure of the automatic daily e-mail-generated reports for five of the 37 (approximately 14%) FAMIS-WCF database audit logs sampled for testing. These failures occurred between February 17, 2022 through February 25, 2022.

During this time, DISA personnel with responsibility over maintaining and reviewing database audit logs had to manually generate reports from the database for analysis and review. However, DISA personnel failed to consistently generate and perform timely review over the necessary audit log reports during this time.

Effect: By not reviewing FAMIS-WCF database audit logs in a timely manner, DISA personnel may not be aware of potential issues that could affect the FAMIS-WCF database. Those issues may affect the integrity and availability of the FAMIS-WCF database, as well as the security baseline. Untimely audit log reviews may result in inappropriate or malicious actions remaining undetected for an extended period, which may hinder DISA's ability to initiate prompt corrective action.

Recommendations: Kearney recommends that DISA perform the following:

1. Update FAMIS-WCF procedural documentation to include supplemental review procedures or alerts when the FAMIS-WCF database fails to generate audit log files automatically.
2. Continue to implement the documented review process and retain evidence of the review of FAMIS-WCF database logs for third-party review.
3. Develop and implement a QC process over the FAMIS-WCF database logging and monitoring review process. The QC process should include procedures to ensure FAMIS-WCF database logs are generated and reviewed within prescribed timelines.

I. Incomplete Complementary User Entity Controls 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 System and Organization Controls (SOC) report. In FY 2022, each service organization provided DISA management with a SOC 1®, Type 2, *Report on an 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 certain controls (i.e., complementary user entity controls [CUEC]) to achieve the overall control objectives and create a secure computing environment. Specifically, 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 DPAS for logistics and property management services; DLA's Wide Area Workflow (WAWF) for management of goods and services; DFAS's 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 Defense Manpower Data Center's (DMDC) Defense Civilian Personnel Data System (DCPDS) for processing payroll affecting civilian human resource transactions.

Condition: DISA has not implemented all of the CUECs required by its service organizations. Based on a subset of high-risk CUECs (e.g., cross-system segregation of duties [SD], periodic access reviews, and removals) required by DISA's service organizations, examples of control deficiencies indicating CUECs that DISA has not fully implemented included:

- DISA did not develop cross-system SD documentation to detail conflicts that may occur when personnel obtain access to multiple systems utilized by DISA to include, but not be limited to, DAI, DPAS, WAWF, DCAS, DCPS, DDRS, and DCPDS
- DISA did not perform periodic reviews of DISA users for the DCPS application
- DISA did not consistently remove or disable access to DISA users of the DAI and DPAS applications upon their separation from the agency.

Cause: Although DISA was aware of the requirements for implementing the CUECs and had begun implementation, it had not finalized implementation of all CUECs as of the end of the FY 2022 financial statement audit. Throughout FY 2022, DISA refined its existing process regarding implementation of all CUECs identified within each service organization and implemented a QC review over the process. Additionally, due to the large number of CUECs, DISA established a three-year schedule and executed it to test CUECs based on level of risk.

Effect: As SOC 1®, Type 2 reports address the effectiveness of controls related to the user entity's financial reporting, ineffective controls/control objectives (i.e., Access Controls, Security Management, and Configuration Management) increase the risk of negative impact to the confidentiality, integrity, and availability of data supporting DISA's financial statements.



Ineffective controls/control objectives may result from DISA's failure to implement internal controls to address all required CUECs.

Recommendations: Kearney recommends that DISA perform the following:

1. Finalize and implement the 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.
2. Implement all CUECs identified within each service organization's SOC 1®, Type 2 report.
3. Implement a QC review over the CUEC process.

* * * * *

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) 2021 financial statements, we noted several issues that were related to internal control over financial reporting. The statuses of the FY 2021 internal control findings are summarized in *Exhibit 3*.

Exhibit 3: Status of Prior-Year Findings

Control Deficiency	FY 2021 Status	FY 2022 Status
Fund Balance with Treasury	Material Weakness	Material Weakness
Accounts Receivable/Revenue/ Accounts Payable/Expense	Material Weakness	Not Applicable (N/A)
Property, Plant, and Equipment	N/A	Material Weakness
Budgetary Resources	Material Weakness	N/A
Financial Reporting	Significant Deficiency	Significant Deficiency
Information Technology	Significant Deficiency	Significant Deficiency

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 Department of 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. 22-01, *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, 2022 and the related notes to the financial statements, which collectively comprise DISA WCF's basic financial statements, and we have issued our report thereon dated December 15, 2022.

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether DISA WCF's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of the financial statement, 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 DISA WCF. However, providing an opinion on compliance with those provisions was not an objective of our audit; accordingly, we do not express such an opinion. The results of our tests disclosed an instance of noncompliance or other matter that is required to be reported under *Government Auditing Standards* and OMB Bulletin No. 22-01 and which is described in the accompanying **Schedule of Findings** as Item I.

The results of our tests of compliance with FFMIA disclosed no instances in which DISA WCF's financial management systems did not comply substantially with the Federal financial management system's requirements, applicable Federal accounting standards, or application of the United States Standard General Ledger at the transaction level.

DISA WCF's Response to Findings

Government Auditing Standards requires the auditor to perform limited procedures on DISA WCF's response to the findings identified in our audit and described in the accompanying Agency Financial Report (AFR). DISA WCF concurred with the findings identified in our engagement. DISA WCF's response was not subjected to the other auditing procedures applied in the audit of the financial statements; accordingly, we express no opinion on the response.



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 *Government Auditing Standards* and OMB Bulletin No. 22-01 in considering the entity's compliance. Accordingly, this communication is not suitable for any other purpose.

A handwritten signature in blue ink that reads "Kearney & Company". The signature is written in a cursive, flowing style.

Alexandria, Virginia
December 15, 2022

Schedule of Findings

Noncompliance and Other Matters

I. The 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 Federal Managers' Financial Integrity Act of 1982 (FMFIA). FMFIA and OMB Circular A-123 require agencies 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 the Federal 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 two 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)
 - Property, Plant, and Equipment (PP&E)
- Significant Deficiencies:
 - Financial Reporting
 - Information Technology (IT).

DISA Management Comments to Auditor's Report



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

Mr. Kelly Gorrell
Kearney & Company
1701 Duke Street, Suite 500
Alexandria, VA 22314

Mr. Gorrell:

DISA acknowledges receipt of Kearney & Company's draft audit report for DISA's FY 2022 Working Capital Fund (WCF) financial statements.

We acknowledge the auditor-identified findings in the following key areas: 1) Fund Balance with Treasury and 2) Property, Plant and Equipment, each of which, in the aggregate, are considered material weaknesses. We also acknowledge the auditor-identified findings in the following key areas: 1) Financial Reporting and 2) Information Technology, each of which, in the aggregate, are considered significant deficiencies.

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

DIAZ.ALEXIS. Digitally signed by
DIAZ.ALEXIS. [REDACTED]
Date: 2022.12.15 16:48:06
-05'00'

ALEX DIAZ
Director, Accounting Operations
and Compliance