

**Defense Information Systems Agency
Working Capital Fund
Agency Financial Report
Fiscal Year 2024**



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, 2024. These 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. As the agency head, I have assessed the financial and performance data in this report and can rely on the completeness and reliability of the data. The results and response to this assessment are further discussed throughout this letter.

In FY 2024, DISA continues to be a trusted partner throughout the Department of Defense (DoD), leading the way in providing information technology (IT) and telecommunication support to our warfighters. DISA is optimizing the DoD's network, by modernizing the infrastructure, finding opportunities to leap ahead, and divest of legacy. The agency is committed to enhancing protection against sophisticated threats, while improving user access to cloud applications and migrations to the DoD365 environment. As a combat support agency, DISA continues to support global DoD missions, including those in Ukraine, Israel, and Haiti.

DISA's strategy for FY 2025-2029, DISA Next, outlines how the agency is solving enterprise-level, hard, and complex IT and telecommunications problems. Our first priority is to simplify the network with large-scale adoption of a common IT environment. Consolidating combatant commands, defense agencies, and field activities is also a key step in providing a DoD-wide warfighting information system. Second, we must develop a fully functional DoD enterprise cloud environment and enable secure cloud access to provide relevant tools that DoD customers need to fully realize cloud capabilities. The third priority is to integrate our Identity, Credential, Access Management (ICAM), and Zero trust capabilities with our common IT and club environment.

This year, we have continued to make improvements in our financial processes based on feedback by our independent public accounting (IPA) firm Kearney & Company. The IPA reported significant deficiencies, which DISA is addressing through mitigating controls, specifically in Fund Balance with Treasury, budget clearing account reconciliation and reporting processes, and statement of difference reconciliation and reporting processes. DISA's WCF continues to evolve our financial processes, through updated internal controls (such as ICAM) that improve accuracy and efficiency for better decision making. DISA can provide reasonable assurance that internal controls over financial reporting, operations, and compliance are operating effectively as of Sept. 30, 2024. DISA's WCF has established corrective action plans to address the significant deficiency findings on DISA's WCF financial statements. DISA will continue to gain efficiencies by expanding our usage of automation. 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, appearing to read 'Paul T. Stanton'.

PAUL T. STANTON, Ph.D.
Lieutenant General, USA
Director

Table of Contents

Management’s Discussion and Analysis	1
Context for the Financial Information in the MD&A.....	2
Analysis of Financial Statements.....	11
Analysis of Systems, Controls, and Legal Compliance.....	21
Forward-Looking Information.....	33
Principal Statements	34
Notes to the Principal Statements	39
Required Supplementary Information	57
Deferred Maintenance and Repairs Disclosures.....	58
Other Information	59
Management Challenges.....	61
Payment Integrity.....	68
DoD Office of Inspector General (OIG) Audit Report Transmittal Letter	69
Independent Auditor’s Report	72
DISA Management Comments to Auditors Report	97
Appendix A	99

DISA Working Capital Fund

Management's Discussion and Analysis

Fiscal Year 2024, Ending Sept. 30, 2024

The Defense Information Systems Agency (DISA) is pleased to present a Management Discussion and Analysis (MD&A) to accompany its fiscal year (FY) 2024 financial statements and footnotes. The key sections within this MD&A include the following:

- 1. Context for the Financial Information in the MD&A**
- 2. Analysis of Financial Statements**
- 3. Analysis of Systems, Controls, and Legal Compliance**
- 4. Forward-Looking Information**

1. Context for the Financial Information in the MD&A

History and Enabling Legislation

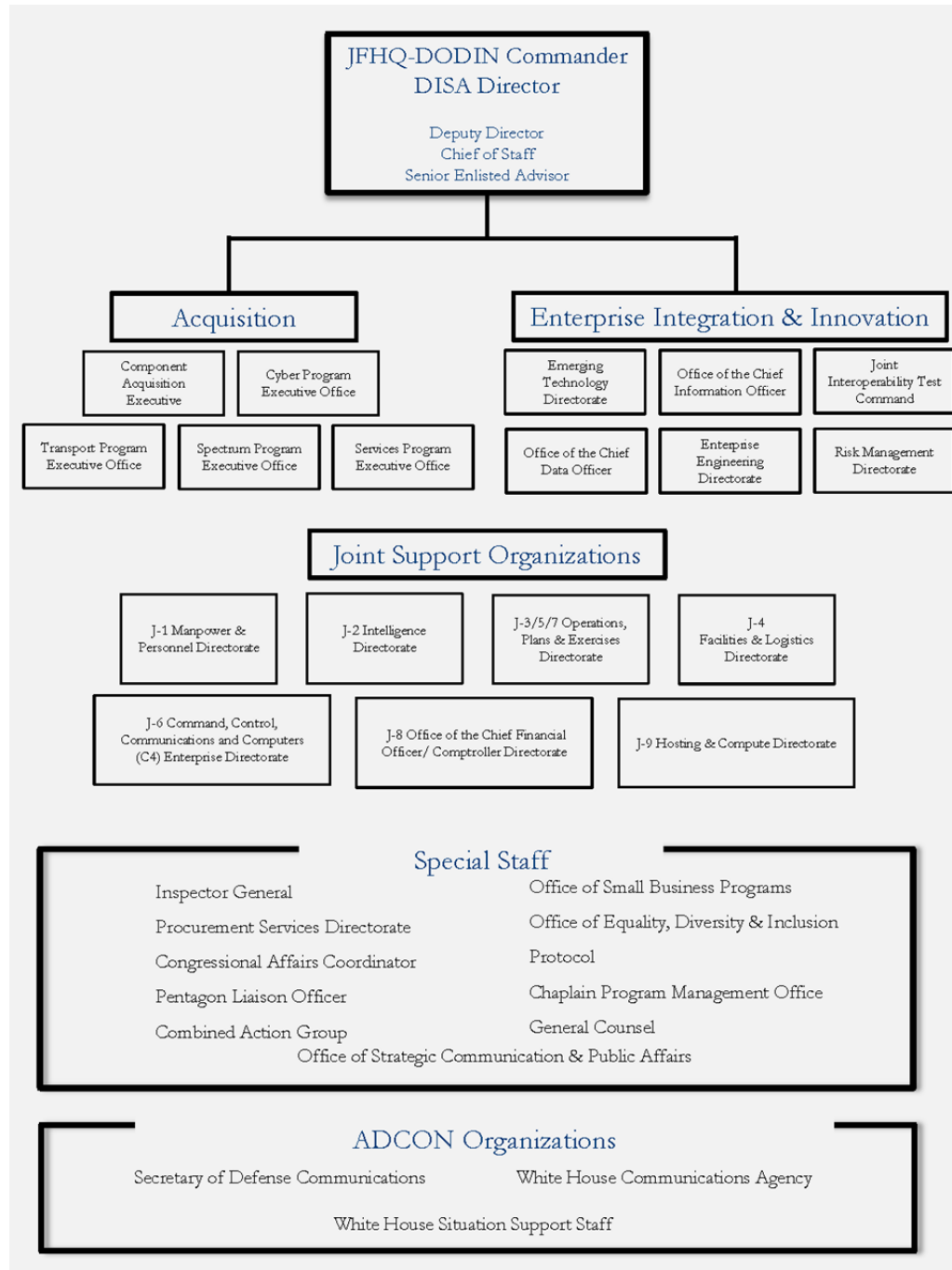
DISA, a combat support agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support of joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations. DISA implements the Secretary of Defense's Defense Strategic Guidance and reflects the Department of Defense (DoD) Chief Information Officer's (CIO) Capability Planning Guidance. 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, 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.

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 (NCR). 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 August 2024 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.

In accordance with Statement of Federal Financial Accounting Standards (SFFAS) 47, DISA Working Capital Fund (WCF) does not have any consolidation or disclosure entities that are required to be disclosed within these notes. Although component reporting entities of the federal government may significantly influence each other, component reporting entities are subject to the overall control of the federal government and operate together to achieve the policies of the federal government and are not considered related parties. Therefore, component reporting entities need not be disclosed as related parties by other component reporting entities. Disclosure entities are not consolidation entities. Disclosure entities may provide the same or similar goods and services that consolidation entities do but are more likely to provide them on a market basis.

DISA's Defense Working Capital Fund (DWCF)

DISA operates a DWCF budget. The 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 three main programs that make up the One Fund: Telecommunications Services (TS) (PE55), Enterprise Acquisition Services (EAS) (PE56) and Computing Services (CS) (PE54). These are the programs that make up the Statement of Net Cost.

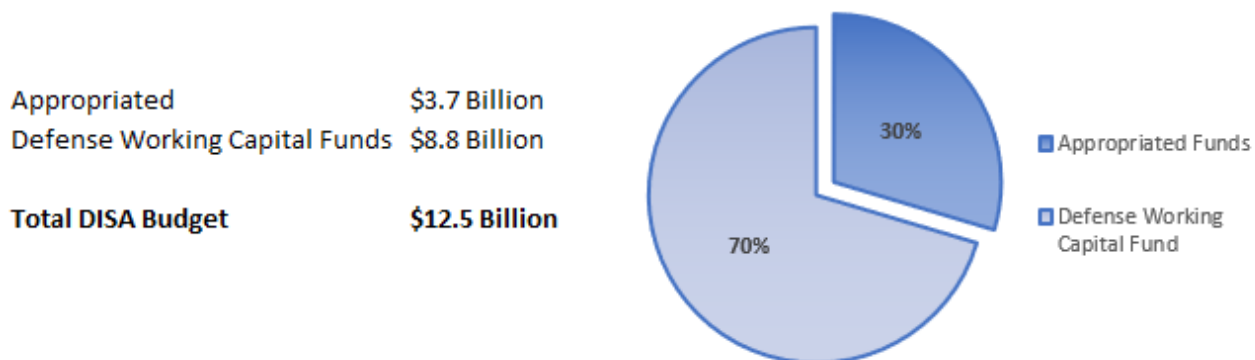
The major element of the TS (PE55) component is the Defense Information Systems Network (DISN), which provides interoperable telecommunications connectivity and accompanying services that allow the department to plan and operate both day-to-day business and operational missions through the dynamic routing 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 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 CS (PE54) 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 17 mainframes; approximately 9,000 servers; 110,000 terabytes of storage data; 3,600 network devices and approximately 219,000 square feet of raised floor.

Resources: DISA is a combat support agency of the DoD with a \$12.5 billion annual budget.

BUDGET



Global Presence

DISA is a global organization of approximately 7,500 civilian employees; 1,600 active-duty military personnel from the Army, Air Force, Navy, and Marine Corps; and over 11,000 defense contractors. This data is as of August 2024. 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.

DISA is the combat support agency entrusted with the Defense Department's information system network. It is our responsibility to transform and integrate our capabilities and services to best support the DoD. The strategic planning framework aligns agency day-to-day efforts to the National Defense Strategy (NDS).

The first two strategic imperatives and four operational imperatives describe DISA's daily mission. As a combat support agency, DISA is designed and chartered to execute these critical functions. These imperatives align to the NDS priorities and reflect how DISA enables the Defense Department and Joint Force as they deter, defend and campaign.

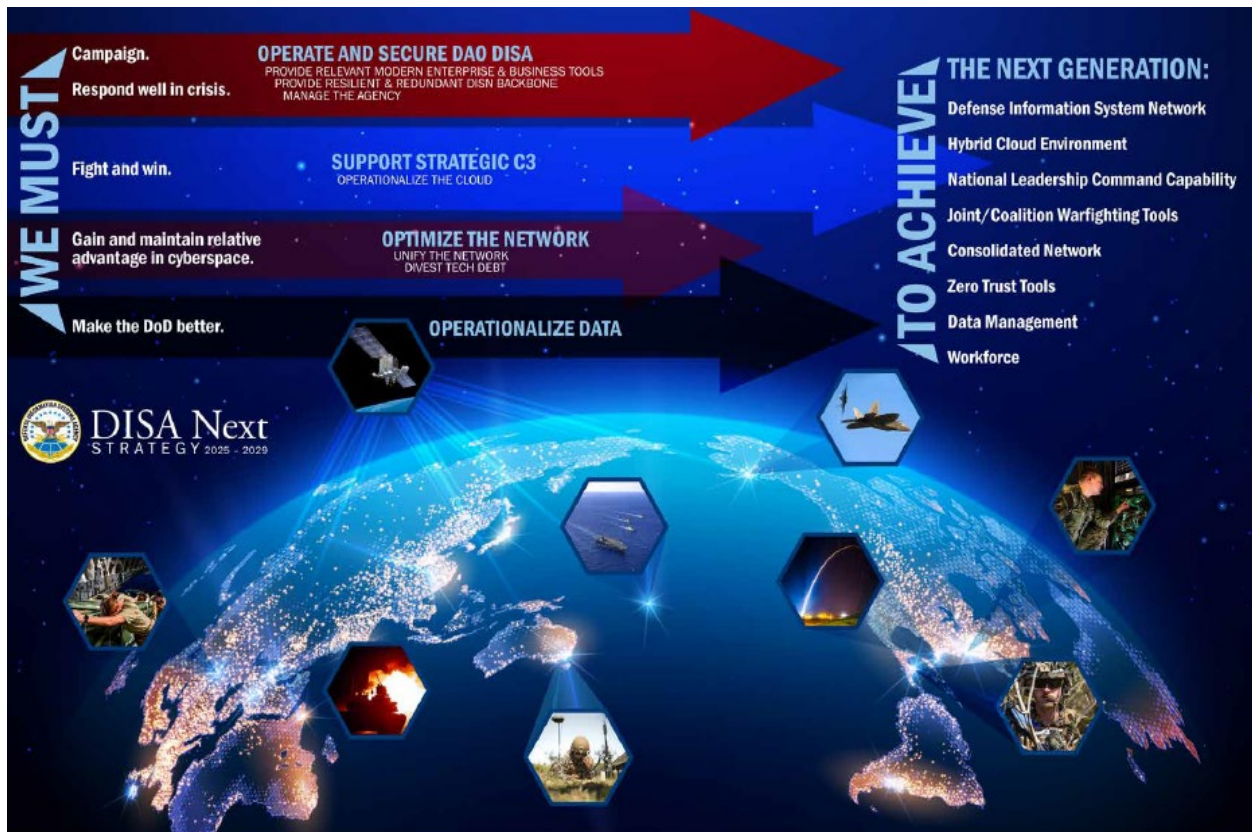
Strategic Imperative 1 is to Operate and Secure the DISA Portion of the DoD Information Network. Operate refers to the 24/7 management of DISA's terrain, whereas secure refers to DISA's responsibility to protect DISA's terrain, data at rest and data in transit.

The first Operational Imperative is to provide relevant, modern enterprise and business tools. DISA must provide state of the art capabilities that will not only meet current requirement but will posture their customers to take advantage of emerging capabilities that provide competitive advantages in a contest environment. The second Operational Imperative is to provide resilient and redundant Defense Information System Network backbone. To ensure there are no breaks in service and that all traffic arrives at its destination unimpeded, it is critically important that DISA build survivability into the DISN. The third Operational Imperative is to manage the agency. DISA's administrative activities that are

crucial in this endeavor include governance, facility management, human capital initiatives and internal processes.

Strategic Imperative 2 is to Support Strategic Command, Control and Communications. DISA is key to supporting the systems, capabilities, networks and processes that enable command and control and allow senior leaders to communicate securely across the globe. The fourth Operational Imperative is to Operationalize the Cloud. DISA's cloud service will be operationalized, meaning the agency will provide a secure cloud environment so warfighters may access data at the breadth, width and speed of modern combat operations.

DISA Approach as outlined in the FY 2025-2029 Strategic Plan include:



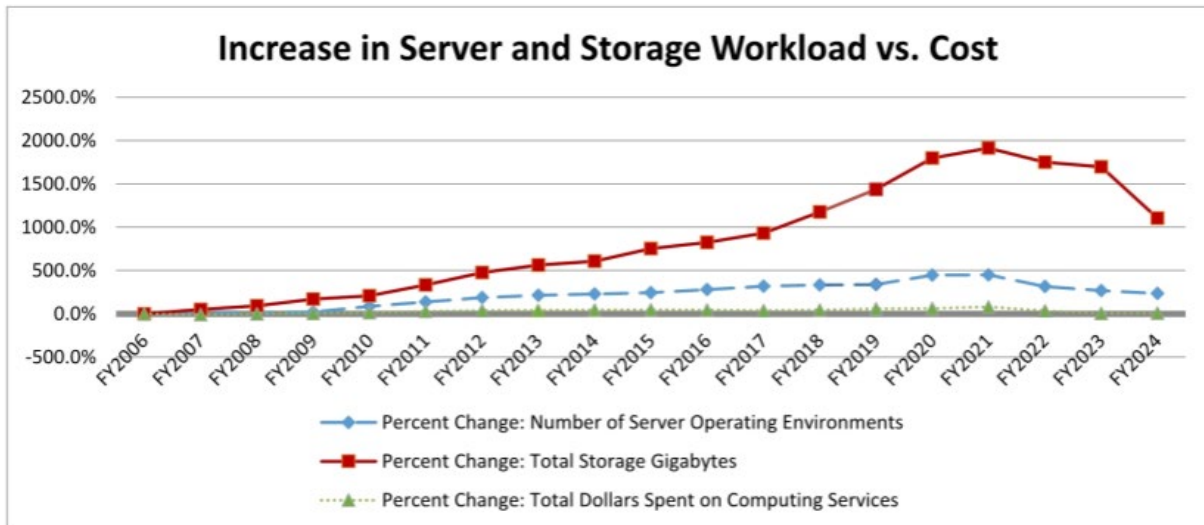
The overarching drive of the DISA Next Strategy is that DISA Must: Campaign; Respond well in crisis, fight and win; gain and maintain relative advantage in cyberspace; and make the DoD better. This is achieved through the strategic imperatives and their coordinating operational imperatives described. The imperatives suggest forward motion toward the future, arriving at the goals of next generation DISN, hybrid cloud environment, national leadership command capability, joint/coalition warfighting tools, a consolidated network, zero-trust tools, data management, and workforce.

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

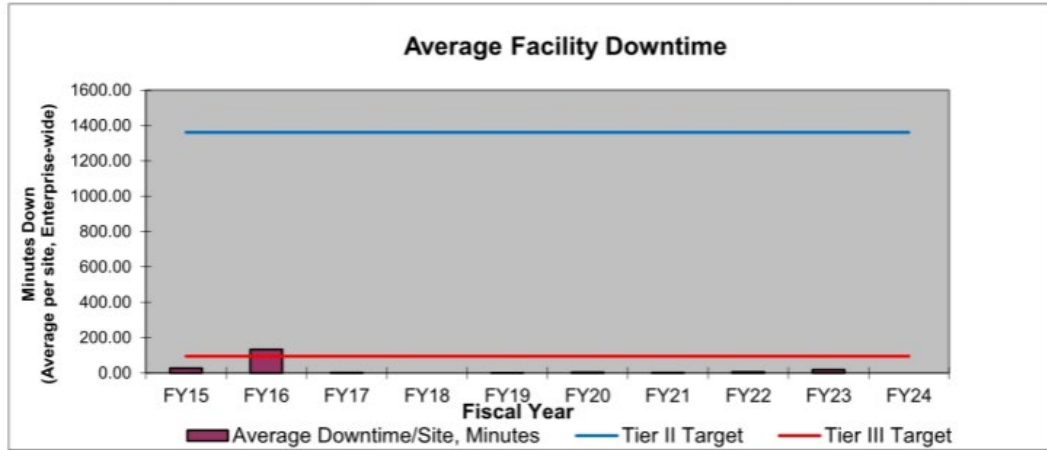
The table below represents the increased demand for DISA’s server and storage computing services, which has grown significantly since FY 2006. Since that year, the number of customer driven server operating environments has increased by 267 percent, and total storage gigabytes have increased by 1,698 percent. Over the same timeframe, the cost to deliver all computing services has increased by only 8 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 (PE54) 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

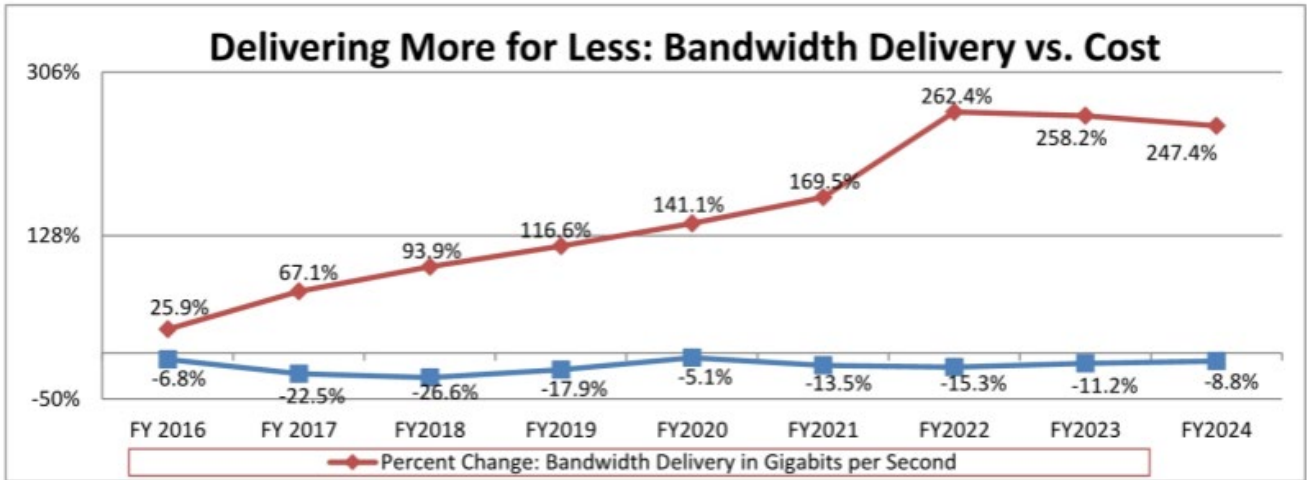


The second metric, “Capacity Service Contract Equipment Availability,” represents DISA’s equipment availability by technology, i.e., how well DISA is executing its responsibilities exclusive of factors outside the agency's control such as last-mile communications issues, base power outages, or the like. 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%	100%
Storage	99.95%	>99.95%	99.999%
Communications Devices	99.95%	>99.95%	99.999%

The Telecommunications Services (PE55) 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 Department of Defense Information Network (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 2016, DISA has increased transport bandwidth delivery capacity 247.4 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 11.2 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 2024 Operational Goal	FY 2025 Operational Goal	FY 2026 Operational Goal
Non-Secure Internet Protocol Router Network access circuit availability	98.5%	98.50%	98.50%
Secure Internet Protocol Router Network latency (measurement of network delay) in the continental United States	<= 100 milliseconds	<= 100 milliseconds	<= 100 milliseconds
Optical Transport	99.50%	99.50%	99.50%

The EAS (PE56) business area is the department’s ideal source for procurement of best-value and commercially competitive IT. EAS provides contracting services for IT and telecommunications acquisitions from the commercial sector and contracting support to the DISN programs, as well as to other DISA, DoD, and authorized non-defense customers. These contracting services are provided through DISA’s DITCO and include acquisition planning, procurement, tariff surveillance, cost and price analyses, and contract administration. These services provide end-to-end support for the mission partner.

Figure 3- EAS Performance Measures

SERVICE OBJECTIVE	FY 2024 Estimated ACTUAL	FY 2025 Operational Goal*	FY 2026 Operational Goal*
Percent of total eligible contract dollars completed	82.4%	73.00%	73.00%
Percent of total eligible contract dollars awarded to small businesses	21.43%	25.00%	25.00%

*FY 2025 and FY 2026 goals for percent of total eligible contract dollars competed are estimates based on the released FY 2024 goal. The goals have not yet been released by the Defense Procurement Acquisition Policy (DPAP).

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. DISA’s AFR will be published at <https://www.disa.mil/about/legal-and-regulatory/budget-and-performance-reports> by Nov. 15, 2024.

2. Analysis of Financial Statements

Background

Defense Information Systems Agency (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.

DISA has an established audit committee to oversee 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. DISA Audit Committee is composed of three members who are not part of DISA. The current mission of 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.

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

DISA WCF Status of Fund Balance with the U.S. Department of the Treasury (Line 1.A Unobligated Balance Available, see Footnote 2. Fund Balance with Treasury (FBWT)) reflects the results of budget execution that saw the fund increase \$210.4 million for a total of \$581 million on its unobligated balance available, as compared with the fourth quarter of FY 2023.

- The Statement of Net Cost reflects a gain through the fourth quarter of FY 2024 of \$26.7 million and includes the non-recoverable depreciation expense for network equipment transferred to DISA WCF Telecommunication Services Enterprise Acquisition Services (TSEAS).
- The Statement of Budgetary Resources, New Obligations and Upward Adjustments increased by \$1.2 billion, in comparison with the fourth quarter of last year.
- Cash levels remained positive through the fourth quarter of FY 2024 at 15 days operating cash.
- 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 2024 reported balances and the fourth quarter of FY 2023. Balances that have the same underlying explanation between budgetary and proprietary accounts are explained from the proprietary perspective and referenced from the budgetary perspective.

STATEMENT OF NET COST

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

Gross Cost - Gross Cost totaling \$8.8 billion increased \$702.3 million (9 percent) between the fourth quarter of FY 2023 and the fourth quarter of FY 2024. In accordance with regulations and guidance, this reflects the full cost of DISA WCF to include recoverable and non-recoverable costs.

DISA WCF re-evaluated the presentation of the SNC and presented as one consolidated program for the purpose of financial reporting.

Figure 4- Gross Cost

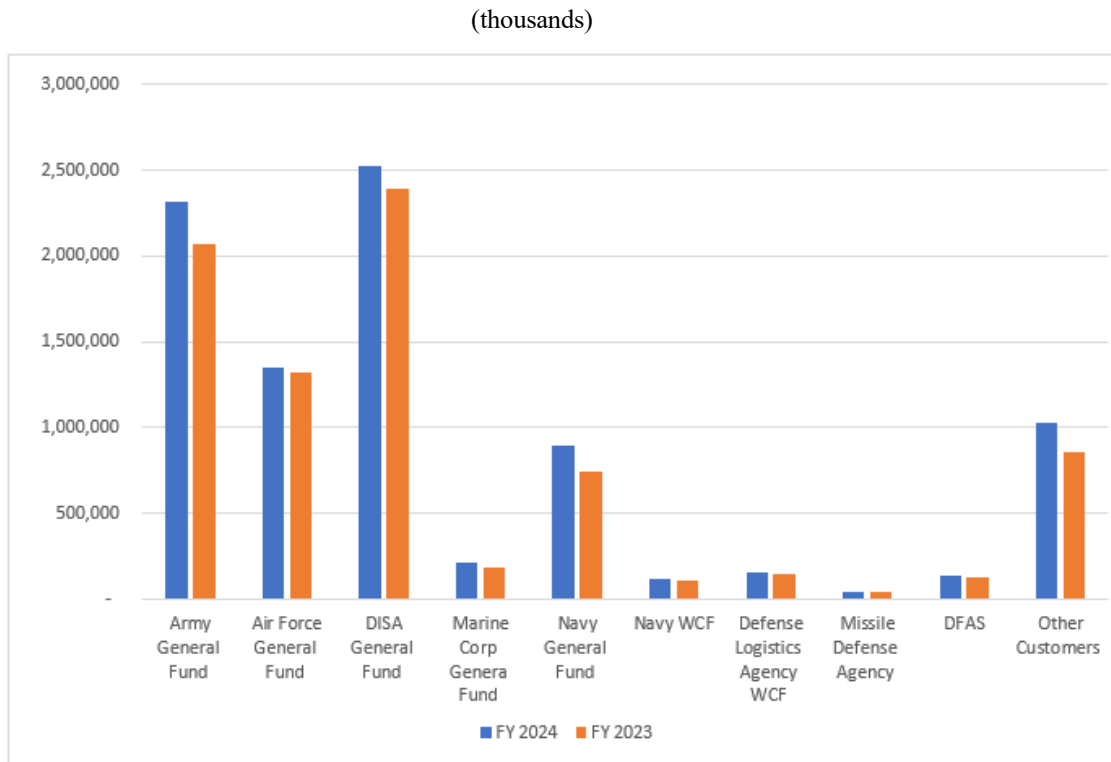
(thousands)

	9/30/2024	9/30/2023	Inc./(Dec.)	% Chg.
Legacy CS	\$ -	\$ (7,556)	\$ 7,556	-100%
One Fund	8,801,400	8,105,635	695,765	9%
Component	(35,174)	(34,154)	(1,020)	3%
Total	\$ 8,766,226	\$ 8,063,925	\$ 702,301	9%

Earned Revenue - Earned Revenue totaling \$8.8 billion increased \$796.8 million (10 percent) between the fourth quarter of FY 2023 and the fourth quarter of FY 2024.

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

The bar chart below reflects earned revenue per customer for FY 2024 and FY 2023.



Net Cost of Operations – Net Cost of Operations decreased \$94.5 million (139 percent) between the fourth quarter of FY 2023 and the fourth quarter of FY 2024 due to the increase in earned revenue of \$796.8 million as well the increase in gross cost of \$702.3 million between fiscal years.

Figure 5- Net Cost of Operations

(thousands)

	9/30/2024	9/30/2023	Inc./(Dec.)	% Chg.
Legacy CS	\$ -	\$ (8,079)	\$ 8,079	-100%
One Fund	8,428	110,015	(101,587)	-92%
Component	(35,174)	(34,154)	(1,020)	3%
Total	\$ (26,746)	\$ 67,782	\$ (94,528)	-139%

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

BALANCE SHEET

The Balance Sheet presents amounts available for use by DISA (assets) against amounts owed (liabilities) and amounts that compose the difference (net position).

Assets

Total assets of \$2.8 billion composed of primarily Fund Balance with Treasury (\$431.2 million); Intragovernmental Accounts Receivable (\$858.3 million); and General and Right-to-Use Property, Plant, and Equipment (PP&E) (\$1.5 billion).

Fund Balance with Treasury - Fund Balance with Treasury Inception to Date (ITD) Balance increased \$126.1 million (41 percent) over last year. The following chart displays fiscal year to date (FYTD) new cash flow from current year operations (collections less disbursements) reported to Treasury for FY 2024 and FY 2023, as reflected in the monthly 1307 Cash Flow report, presented in a comparative manner.

Figure 6- Fund Balance with Treasury

(thousands)

	9/30/2024	9/30/2023	Inc./Dec.	% Chg.
Legacy CS Beginning Balance	\$ -	\$ 49,946	\$ (49,946)	-100%
Legacy CS YTD	-	745,193	(745,193)	-100%
Legacy CS Total	-	795,139	(795,139)	-100%
One Fund Beginning Balance	305,142	288,272	16,870	6%
One Fund YTD	126,056	(778,269)	904,325	-116%
One Fund Total	431,198	(489,997)	921,195	-188%
Total Beginning Balance	305,142	338,218	(33,076)	-10%
YTD	126,056	(33,075)	159,131	-481%
Total ITD Balance	\$ 431,198	\$ 305,143	\$ 126,055	41%

- The \$431.2 million cash balance on Sept. 30, 2024, is composed of a \$305.1 million current year beginning balance and a FYTD \$126.1 million increase from current year operations (includes capital outlays).
- The current year \$126.1 million increase in fund balance results in a \$115.3 million positive variance when compared with the \$10.8 million forecasted decrease, as reflected in the Budget Executive Summary Cash Plan. Actual disbursements were \$181.2 million over plan, and actual collections were \$296.5 million over plan.
- The WCF increase in cash from operations of \$126.1 million (41 percent) from Sept. 30, 2023, to Sept. 30, 2024, is consistent with normal business trends for accounts receivable and accounts payable fluctuations along with increases in Telecommunications Contracts compared to FY 2023.
- The \$431.2 million WCF ITD cash balance represents approximately 15 days of cash on hand on Sept. 30, 2024, which was formulated by dividing \$431.2 million by the daily cash calculation amount of \$28.7 million.
- Amounts recorded in the general ledger for 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.
- DISA WCF ITD FBWT balance remains a key figure in evaluating the “health” of the fund.

Accounts Receivable, Net - Accounts Receivable decreased \$14 million (2 percent). The largest decrease was within the intragovernmental receivables and is due to normal business trends.

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

Figure 7- Accounts Receivable, Net

(thousands)

	9/30/2024	9/30/2023	Inc./Dec.	% Chg.
One Fund				
Intragov.	\$ 858,311	\$ 872,973	\$ (14,662)	-2%
Public	1,579	875	704	80%
Total	\$ 859,890	\$ 873,849	\$ (13,958)	-2%

General and Right-to-Use Property, Plant, and Equipment, Net – DISA WCF general and right-to-use PP&E consists primarily of equipment used by DISA organizations to deliver computing services to customers in DISA Computing Ecosystem and telecommunications services across the Defense Information Systems Network (DISN).

Figure 8- General and Right-to-Use Property, Plant & Equipment, Net

(thousands)

	9/30/2024	9/30/2023	Inc./Dec.	% Chg.
One Fund	\$ 1,486,977	\$ 1,011,565	\$ 475,412	47%
Total	\$ 1,486,977	\$ 1,011,565	\$ 475,412	47%

- PP&E increased \$475.4 million (47 percent) and is mainly due to the increase in Other PP&E. The increase is due to newly identified assets per SFFAS 54 guidelines to record leased assets. The increase in construction-in-progress (CIP) is due to an increase in receipts for capital purchases related to the DISN, which was previously funded under the GF. Decreases were mainly due to general equipment and assets previously under capital lease.
- Non-recoverable depreciation expenses decreased \$35.2 million (19 percent) between fiscal years. This decrease is a result of non-recoverable depreciation associated with DISA GF general property, plant, and equipment transferred to the DISA WCF.

Figure 9- General and Right-to-Use PP&E-Net Book Value

(thousands)

	9/30/2024	9/30/2023	Inc./Dec.	% Chg.
WCF NBV	\$ 1,486,977	\$ 1,011,565	\$ 475,412	
One Fund DPAS Values	458,105	436,211	21,894	5%
Optical Transport Network	61,785	62,208	(423)	-1%
Fiber IRUs	-	26,599	(26,599)	-100%
Joint Regional Security Stacks	132,814	156,419	(23,605)	-15%
TSEAS Assets Pending	141,544	126,250	15,294	12%
Fed Leases	506,544	-	506,544	100%
Multiprotocol Label Switching	1,924	11,957	(10,033)	-84%
Subtotal	1,302,716	819,644	483,072	59%
Non-Recoverable Depreciation	147,481	182,640	(35,159)	-19%
NBV of Remaining Programs	\$ 36,780	\$ 9,281	\$ 27,499	296%

Other Assets – Advances and prepayments increased \$2 million (100 percent) due to an increase in prepaid projects with DFAS.

Figure 10- Other Assets

		(thousands)			
		9/30/2024	9/30/2023	Inc./Dec.	% Chg.
One Fund					
Public	\$	2,000	\$ -	\$ 2,000	100%
Total	\$	2,000	\$ -	\$ 2,000	100%

Liabilities

Total liabilities of \$1.4 billion is composed primarily of intragovernmental accounts payable (\$37.7 million), intragovernmental other liabilities (\$3.4 million), non-federal accounts payable (\$829.8 million), federal employee benefits (\$52.3 million), veteran, pensions, and post employment-related benefits (\$4.7 million), and non-federal other liabilities (\$500 million).

Total Liabilities Not Covered by Budgetary Resources – Total liabilities not covered by budgetary resources increased \$499.8 million (8626 percent) and consists of other liabilities. The increase in other liabilities is due to an adjustment being made for FY 2024 to comply with the implementation of SFFAS 54-Leases. A leased asset is recorded when the lessee takes control over the use of equipment. The adjustment is prepared to record the leased asset for FY 2024 but was not done in FY 2023.

Figure 11- Total Liabilities Not Covered by Budgetary Resources

		(thousands)			
		9/30/2024	9/30/2023	Inc./Dec.	% Chg.
One Fund	\$	505,612	\$ 5,794	\$ 499,818	8626%
Total	\$	505,612	\$ 5,794	\$ 499,818	8626%

Total Liabilities Covered by Budgetary Resources – Total liabilities covered by budgetary resources decreased \$78.4 million (8 percent). The largest portion of the balance is made up of IT contracts. The table below compares current year with prior year liabilities covered by budgetary resources and includes the public accounts payable balances.

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.

Figure 12- Total Liabilities Covered by Budgetary Resources

		(thousands)			
		9/30/2024	9/30/2023	Inc./Dec.	% Chg.
Legacy CS	\$	-	\$ 1,957	\$ (1,957)	-100%
One Fund		924,261	1,000,735	(76,474)	-8%
Total	\$	924,261	\$ 1,002,692	\$ (78,431)	-8%

Other Liabilities - Other Liabilities increased \$453.5 million (910 percent), primarily driven by the adjustment being made for FY 2024 to comply with the implementation of SFFAS 54.

Figure 13- Other Liabilities

(thousands)

	9/30/2024	9/30/2023	Inc./ (Dec.)	% Chg.
Legacy CS				
Public	\$ -	\$ 3,663	\$ (3,663)	-100%
One Fund				
Intragov.	3,373	2,738	635	23%
Public	499,976	43,426	456,550	1051%
Total				
Intragov.	3,373	2,738	635	23%
Public	499,976	47,089	452,887	962%
Total	\$ 503,349	\$ 49,827	\$ 453,522	910%

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 decreased \$13.2 million (12 percent) primarily in Telecommunications Services, specifically Transport Services. This is a result of less current year transfers-in of general property, plant, and equipment along with associated non-recoverable depreciation from DISA GF without reimbursement in FY 2024. Additionally, there were current year reversals of prior year activity that also contributed to the change.
- Imputed financing costs absorbed by others increased \$9.7 million (27 percent) due to the current fiscal year increase in employee imputed cost for life, health, and retirement.
- Net Cost of Operations decreased \$94.5 million (139 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)

	9/30/2024	9/30/2023	Inc./.(Dec.)	% Chg.
Legacy CS				
Obligations Incurred	\$ -	\$ (46,801)	\$ 46,801	-100%
Unobligated Balances	-	779,774	(779,774)	-100%
Contract Authority	-	(39,576)	39,576	-100%
Unfilled Customer Orders	-	-	-	0%
Net Outlays	-	6,607	(6,607)	-100%
One Fund				
Obligations Incurred	9,257,000	8,090,199	1,166,801	14%
Unobligated Balances	610,760	(409,209)	1,019,969	-249%
Contract Authority	160,280	152,616	7,664	-5%
Unfilled Customer Orders	3,563,140	873,053	2,690,087	308%
Net Outlays	(126,056)	26,468	(152,524)	-576%
Total				
Obligations Incurred	9,257,000	8,043,398	1,213,602	15%
Unobligated Balances	610,760	370,566	240,195	65%
Contract Authority	160,280	113,040	47,240	42%
Unfilled Customer Orders	3,563,140	873,053	2,690,087	308%
Net Outlays	\$ (126,056)	\$ 33,075	\$ (159,131)	-481%

New Obligations and Upward Adjustments (line 2190) - Obligations incurred increased \$1.2 billion (15 percent). The major driver for obligations incurred for DISA WCF was an increase in IT Contracts.

Unobligated Balance, End of Period (line 2490) - The unobligated balance as of Sept. 30, 2024, increased \$240.2 million (65 percent) between fiscal years. This is due to more orders received, specifically in IT compared to obligations incurred. 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 \$47.2 million (42 percent) between fiscal years due to DISA WCF receiving less indefinite contract authority and because the current fiscal year obligations are more than the prior fiscal year.

Unfilled Customer Orders (USSGL 4221) - Unfilled customer orders increased \$2.7 billion (308 percent) between fiscal years due to a reconciling journal voucher that resolved differences between FAMIS and DDRS Budgetary.

Outlays, Net (Line 4190) – Net Outlays decreased \$159.1 million (481 percent) between fiscal years and is reported as negative in this fiscal year due to collections being higher than disbursements.

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. The Unreconciled difference of \$(2) is due to rounding.

Figure 15- Net Cost of Operations

	(thousands)		
DISA WCF 2024	Intragovernmental	With the Public	Total
Net Cost (Revenue) reported on SNC	\$ (8,490,050)	\$ 8,463,304	\$ (26,746)
Components of Net Cost Not Part of Net Outlays:			
Property, plant, and equipment depreciation expense	-	(232,150)	(232,150)
Property, plant, and equipment disposals & revaluations	-	86,651	86,651
Lessee Lease Amortization	-	(142,047)	(142,047)
Property, plant, and equipment	14,322		14,322
Increase/(Decrease) in Assets:			
Accounts receivable, net	(14,662)	704	(13,958)
Advances and Prepayments	-	2,000	2,000
(Increase)/decrease in liabilities:			
Accounts Payable	8,423	77,436	85,859
Lessee Lease Liability	-	114,127	114,127
Federal employee salary, leave, and benefits payable	-	(4,875)	(4,875)
Veterans, pensions, and post employment-related benefits	-	239	239
Advances from Others and Deferred Revenue	(2,000)	-	(2,000)
Other liabilities	(636)	-	(636)
Other Financing Sources:			
Imputed cost	(45,123)	-	(45,123)
Total Components of Net Cost That Are Not Part of Net Outlays	<u>(53,998)</u>	<u>(83,594)</u>	<u>(137,592)</u>
Components of Net Outlays That Are Not Part of Net Cost:			
Acquisition of Capital Assets	-	134,532	134,532
Financing Sources			
Transfers (in)/out without reimbursements	(96,252)	-	(96,252)
Total Components of Net Budgetary Outlays Not Part of Net Cost	(96,252)	134,532	38,280
Total Other Reconciling items	<u>-</u>	<u>-</u>	<u>-</u>
Total Net Outlays	<u>\$ (8,640,300)</u>	<u>\$ 8,514,242</u>	<u>\$ (126,058)</u>
Agency Outlays, Net, Statement of Budgetary Resources			<u>\$ (126,056)</u>
Unreconciled difference			<u><u>\$ (2)</u></u>

Figure 16- Illustrative Table of Key Measures

(thousands)

	9/30/2024	9/30/2023	Inc./Dec.)	% Chg.
COSTS				
Gross Program Costs	\$ 8,766,226	\$ 8,063,925	\$ 702,301	9%
Less: Earned Revenue	8,792,972	7,996,143	796,829	10%
Net Cost of Operations	(26,746)	67,782	(94,528)	-139%
NET POSITION				
Assets:				
Fund Balance with Treasury	431,198	305,143	126,055	41%
Accounts Receivable, Net	859,890	873,848	(13,958)	-2%
Property, Plant & Equipment, Net	1,486,977	1,011,565	475,412	47%
Other	2,000	-	2,000	100%
Total Assets	2,780,065	2,190,556	589,509	27%
Liabilities:				
Accounts Payable	867,523	953,381	(85,858)	-9%
Pension, Post-Employment, [& Veteran] Benefits Payable	56,999	5,276	51,723	980%
Other Liabilities	503,349	49,827	453,522	910%
Other	2,002	2	2,000	100000%
Total Liabilities	1,429,873	1,008,486	421,387	42%
Net Position (Assets minus Liabilities)	\$ 1,350,192	\$ 1,182,070	\$ 168,122	14%

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.

3. Analysis of Systems, Controls, and Legal Compliance

Management Assurances

DISA, Office of the Chief Financial Officer (J8 -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 compliant 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, operations, and compliance.

Based upon this evaluation establishing and integrating internal control into its operations in a risk-based and cost beneficial manner, DISA provides 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

SEP 27 2024

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

SUBJECT: Annual Statement of Assurance Required Under the Federal Managers' Financial Integrity Act (FMFIA) for Fiscal Year (FY) 2024

As Director of the Defense Information Systems Agency (DISA), I recognize DISA is responsible for managing risks and maintaining effective internal controls 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 controls 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, GAO-14-704G, "Standards for Internal Control in the Federal Government." This internal review also included an evaluation of the internal controls around our Security Assistance Accounts (SAA) activities. Based on the results of the assessment, DISA can provide reasonable assurance that internal controls over operations, reporting, and compliance are operating effectively as of September 30, 2024. As of July 31, 2024, there were six categories of material weaknesses (MWs) and Significant Deficiencies (SDs) that DISA is correcting or that have mitigating controls: Accounts Receivable/Revenue; Accounts Payable/Expense; Budgetary Resources; Fund Balance with Treasury; Financial Reporting; and Property, Plant and Equipment (PPE).

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 "*Summary of Management's Approach to 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, 2024.

DISA conducted its assessment of the effectiveness of internal controls over reporting (including internal and external financial reporting) in accordance with OMB Circular No. A-123, Appendix A. The "*Internal Control Evaluation (Appendix C)*" section, provides specific information on how DISA conducted this assessment. This assessment also included an evaluation of the internal controls around our SAA activities. Based on the results of the assessment, DISA can provide assurance that internal controls over reporting (including internal and external reporting) and compliance are operating effectively as of September 30, 2024.

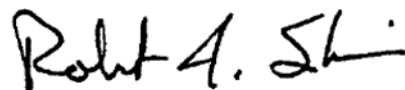
DISA Memo, DIR, Annual Statement of Assurance Required Under the Federal Managers' Financial Integrity Act (FMFIA) for Fiscal Year (FY) 2024

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 also included an evaluation of the internal controls around our activities. Based on the results of this assessment, DISA can provide assurance, except for one non-conformance reported in the *"Significant Deficiencies and Material Weaknesses Template"* 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, 2024.

DISA conducted an assessment of entity-level controls including fraud controls in accordance with the Green Book, OMB Circular No. A-123, the Payment Integrity Information Act of 2019, and GAO Fraud Risk Management Framework. 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 entity-level controls including fraud controls are operating effectively as of September 30, 2024.

DISA hereby reports that we discovered/identified no Anti-Deficiency Act (ADA) violations during our assessments of the applicable processes nor ADA violations have been discovered/identified during our assessments of the applicable processes.

If there are any questions regarding this Statement of Assurance for FY 2024, my point of contact is Mr. Justin Sponseller, at justin.c.sponseller.civ@mail.mil or (614) 692-0686.



ROBERT J. SKINNER
Lieutenant General, USAF
Director

Attachments:
As stated

FY 2024 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 issued the FY 2024 DoD Statement of Assurance Handbook that requires deliverables throughout the reporting cycle. The handbook provides practical guidance to carry out the program. In FY 2023, 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. This emphasis remains in FY 2024; however, there is more focus on integrating an agency Risk Profile that identifies risks and fraud that may potentially impact the agency's strategic objective.

Throughout the process, DISA has provided several templates and deliverables to support not only DISA, but the overall DoD RMIC Program. Throughout 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 2024, at the time of this memorandum, DISA has a potential to close 10 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.

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 adhered 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 provided a structure to identify risk at an enterprise level, as well as at a more granular level. DISA director provided a "tone-at-the-top" memo, which defined management's leadership and commitment towards an effective internal control structure.

The first tier is supported by DISA Senior Assessment Team (SAT), which provides guidance and oversight to the RMIC. 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 Assessable Unit Managers (AUMs) who manage at the program/directorate level within the organization. Each directorate's senior leadership, within each assessable unit, collaborated 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 provided 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) meets during 4th quarter and provides oversight to the internal control program through discussion of results and anticipated outcomes to be reported in the FY 2024 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 negative impact regarding payment integrity and improper payment recovery.

Component Risk Profile:

The risk profile is intended to facilitate strategic decision-making, including informing budget decisions, and enabling efficient resource allocation. DISA's Risk Profile is composed of the highest risks. DISA's risk profile was reviewed and approved by leadership.

Entity-Level Components (ELCs):

The use of Committee of Sponsoring Organizations (COSO) framework, to identify types of evidence to assess emerging technologies in the development of ELCs—including the Component's use of data and system design.

GAO Fraud Risk Management (FRM) Framework Assessment:

To further align the fraud risk management requirements to the GAO FRM Framework, the Fraud Controls Matrix Template has been renamed to the "GAO FRM Framework Assessment".

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. 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 2024. Identified areas of improvements for CARES Act execution include ensuring requirements are aligned with spending plans and ensuring that transactions accurately reflect the Disaster Emergency Fund Code (DEFC).

Fraud Controls:

In FY 2024, 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.

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 2024, 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 FYs 2023 and 2024.

Records Management:

While records management was not an OUSD focal area, 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, the Records Management Self-Assessment (RMSA) for the National Archives and Records Administration (NARA) and the 2021 Federal Electronic Records and Email Management Maturity Model Report (FEREM) for NARA are conducted.

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 DISA SAT, which provides guidance and oversight to the RMIC Program. In FY 2024, 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 coordinated 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 2023 and conducted three additional workshops in the FY 2024 reporting cycle to address risk assessments, testing grids, and letters of assurance. The RMIC team

compiled 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 identifies the following AUMs:

- ✓ Chief Financial Officer/Comptroller (OCFO)
- ✓ Component and Acquisition Executive (CAE)
- ✓ Digital Capabilities and Security Center (DCSC)
- ✓ Chief of Staff (DDC)
- ✓ 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)
- ✓ Manpower & Personnel Directorate (formerly WSD)

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

Identifying Key Controls:

Mandatory testing for all organizations is required to identify the functions performed within their area, in addition to the required testing areas of the Defense Travel System (DTS); Time and Attendance; and 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 documented 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.

Each AU performed 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 likeliness; and residual risk rating, process documentation, and financial statement impact. At the AU level and across the agency, this process developed 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 included 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.

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.

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. Test Plan Description: 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 Type: Test method (inquiry, observation, inspection, or re-performance):
- d. Sample size: Sample size/sampling technique/tolerance rate:
- e. Internal Control Currently in Place 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):**

*LOA information should reflect the data reported on your test grids

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 provided 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 provided 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.

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 provided a detailed analysis, documents the Control Activities identified in the narratives, and included 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 17-Areas of Testing

General Fund	Working Capital Fund	Other
Data Quality Plan	One Fund Trial Balance (Rollforward) Testing	Active Users
Dormant Reviews	One Fund TELECOM Revenue	Departed Users
Year End Obligations	One Fund Non-TELECOM Revenue	Periodic User Access Review (UAR) Testing
GF Trial Balance (Rollforward) Testing	One Fund TELECOM Expenditure	PP&E Activation, CIP, and Transfer Testing
GF Revenue	One Fund Non-TELECOM Expenditure	
GF Expenditure		
CARES Act Testing		

The OUSD FIAR Office led department-wide discussions regarding SSAE 18 reviews and the impact to component financial statements. DISA identified more than 194 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 194 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 2024 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)
- 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)
- Manpower & Personnel Directorate (formerly 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 18-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 19-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 2024, 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 and USSGL compliance in support of a clean audit opinion for the WCF. Additionally, FAMIS deployed the first phase of the future state compliant telecom Business Enterprise Architecture (BEA) solution. This solution enables DISA to begin the sunset activity of legacy telecom systems and provides a compliant and automated solution that complies with DoD policies. FAMIS continued to maintain a strong security posture, receiving a 3-Year Authority to Operate (ATO). Additional capabilities and modernizations deployed into FAMIS included enhanced automation and reconciliation of core cash matching functionalities, enabling DISA's WCF to achieve and maintain its record of zero unmatched disbursements.

This fiscal year also introduced FAMIS-as-a-Service (FaaS). The program is migrating DISA's General Fund business out of the Defense Agencies Initiative (DAI) solution and into FAMIS. The implementation of FaaS across both DISA's WCF and GF will improve operational efficiencies, ensure data integrity, and support compliance of financial standards while leveraging the capabilities of the existing FAMIS baseline. Go-live operational capability for DISA's GF is scheduled in October 2024. Finally, FAMIS began laying the groundwork to migrate 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 continues to standardize 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 four 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.

One example of this modernization is the current undertaking to accredit and stand up a new financial system called the DISA Integrated Management and Execution System (DIMES). DIMES is an Enterprise Performance Management (EPM) solution based on the OneStream platform that supports budgeting, forecasting, financial reporting, and data quality management. By October 2024, DISA will implement the budget execution phase of the project supporting spend planning; subsequent phases to include budget formulation and reporting are targeted to go-live by FY 2026. Once completed, DIMES will be the single platform for users to access budget formulation and execution data for both the GF and WCF and as such, will replace DFMS and DBS (DISA Financial Management System and DWCF Budgeting System).

These advancements will result in increased automation, transparency, access, and control of financial information to support financial managers, mission partners, and higher echelon leaders.

4. 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 is pursuing one Performance Improvement Initiative (PII) related to services offered in the Information Services Activity Group (ISAG) portfolio. This budget includes support of the "Joint Service Provider (JSP) Help Desk Modernization" effort in which tools to improve IT service management performance are being provided on a reimbursable basis. We continue to move forward on several new initiatives, including:

- The implementation of Defense Enterprise office Solutions, which is a commercially provided, cloud-based enterprise service for common communication, collaboration, and productivity services. There has been significant progress towards decommissioning legacy email, video, and audio-conferencing services.
- The Fourth Estate Network Optimization reform initiative includes the convergence of the DoD networks, service desks, and operations centers into a consolidated, secure, and effective environment.
- 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 center footprint, and streamlined cybersecurity infrastructure.
- Includes efforts to modernize the management of the network backbone by moving network management tools to the commercial cloud; moving to cloud-based platforms allowing the network operator to gain access to accurate and real time data which allows more timely decisions to support the warfighter.
- Implementation of the Joint Warfighting Cloud Capability (JWCC) which is a multiple award contract vehicle providing the DoD with direct access to multiple Cloud Service Providers (CSPs) to acquire commercial cloud capabilities and services at the speed of mission-at all classification levels- from headquarter to the tactical edge. Direct awards with the CSPs also allows for streamlined provisioning of cloud services, fortified security, and commercial pricing parity.

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 have yielded a savings of \$717 million over 10 years.

**Defense Information Systems Agency
Working Capital Fund
Principal Statements
Fiscal Year 2024, Ending Sept. 30, 2024**

Department of Defense
Defense Information Systems Agency WCF
Balance Sheet
As of Sept. 30, 2024 and 2023
(\$ in thousands)

Figure 20-Balance Sheet

	<u>2024</u>	<u>2023</u>
Intragovernmental assets:		
Fund Balance with Treasury (Note 2)	\$ 431,198	\$ 305,143
Accounts receivable, Net (Note 3)	858,311	872,973
Total Intragovernmental Assets	<u>1,289,509</u>	<u>1,178,116</u>
Other than intragovernmental assets:		
Accounts receivable, net (Note 3)	1,579	875
General and Right-to-Use property, plant and equipment, net (Note 4)	1,486,977	1,011,565
Advances and prepayments	2,000	-
Total other than intragovernmental assets	<u>1,490,556</u>	<u>1,012,440</u>
Total Assets	<u>\$ 2,780,065</u>	<u>\$ 2,190,556</u>
Liabilities (Note 7)		
Intragovernmental liabilities:		
Accounts payable	\$ 37,717	\$ 46,138
Advances from others and Deferred Revenue	2,000	-
Other Liabilities (Notes 7 and 9)	3,373	2,738
Total intragovernmental liabilities	<u>43,090</u>	<u>48,876</u>
Other than intragovernmental liabilities:		
Accounts payable	829,806	907,244
Federal employee salary, leave, and benefits payable (Note 6)	52,298	47,423
Pension, post-employment, and Veteran Benefits payable (Note 6)	4,701	4,941
Advances from others and Deferred Revenue	2	2
Other Liabilities (Notes 7, 8, and 9)	499,976	-
Total other than intragovernmental liabilities	<u>1,386,783</u>	<u>959,610</u>
Total liabilities	<u>\$ 1,429,873</u>	<u>\$ 1,008,486</u>
Commitments and contingencies (Note 9)		
Net Position:		
Cumulative Results from Operations	\$ 1,350,192	\$ 1,182,070
Total Cumulative Results of Operations (Consolidated)	<u>1,350,192</u>	<u>1,182,070</u>
Total net position	<u>1,350,192</u>	<u>1,182,070</u>
Total liabilities and net position	<u>\$ 2,780,065</u>	<u>\$ 2,190,556</u>

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

**Department of Defense
 Defense Information Systems Agency WCF
 Statement of Net Cost
 For the Years Ended Sept. 30, 2024 and 2023
 (\$ in thousands)**

Figure 21-Statement of Net Cost

Gross Program Costs (Note 12)	2024	2023
Gross Costs (Note 12)	\$ 8,766,226	\$ 8,063,925
Less: Earned Revenue (Note 10)	<u>(8,792,972)</u>	<u>(7,996,143)</u>
Net Cost of Operations	<u><u>\$ (26,746)</u></u>	<u><u>\$ 67,782</u></u>

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

**Department of Defense
 Defense Information Systems Agency WCF
 Statement of Change in Net Position
 For the Years Ended Sept. 30, 2024 and 2023
 (\$ in thousands)**

Figure 22-Statement of Changes in Net Position

CUMULATIVE RESULTS OF OPERATIONS	<u>2024</u>	<u>2023</u>
Beginning Balance	\$ 1,182,070	\$ 1,104,941
Non-exchange revenue	-	2
Transfers-in/out without reimbursement	96,252	109,458
Imputed financing	45,124	35,453
Other	-	(2)
Net Cost of Operations	(26,746)	67,782
Net Change in Cumulative Results of Operations	<u>168,122</u>	<u>77,129</u>
Total Cumulative Results of Operation	<u>1,350,192</u>	<u>1,182,070</u>
Net Position	<u>\$ 1,350,192</u>	<u>\$1,182,070</u>

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

**Department of Defense
Defense Information Systems Agency WCF
Statement of Budgetary Resources
For the Years Ended Sept. 30, 2024 and 2023
(\$ in thousands)**

Figure 23-Statement of Budgetary Resources

	<u>2024</u>	<u>2023</u>
Budgetary Resources		
Unobligated balance from prior year budget authority, Net (Note 11)	\$ 400,324	\$ 107,808
Contract Authority (discretionary and mandatory)	160,280	113,040
Spending Authority from offsetting collections (discretionary and mandatory)	9,307,156	8,193,116
Total Budgetary Resources	<u>\$ 9,867,760</u>	<u>8,413,964</u>
Status of Budgetary Resources		
New obligations and upward adjustments (total)	\$ 9,257,000	\$ 8,043,398
Unobligated balance, end of year		
Apportioned, unexpired accounts	581,001	370,566
Unapportioned, unexpired accounts	29,759	-
Unexpired unobligated balance, end of year	610,760	370,566
Unobligated balance, end of year (total)	<u>610,760</u>	<u>370,566</u>
Total Budgetary Resources	<u>\$ 9,867,760</u>	<u>8,413,964</u>
Outlays, Net		
Outlays, net (total) (discretionary and mandatory) (Note 12)	(126,056)	33,075
Agency Outlays, net (discretionary and mandatory)	<u>\$ (126,056)</u>	<u>\$ 33,075</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 2024, Ending Sept. 30, 2024**

Note 1. Reporting Entity and Summary of Significant Accounting Policies

1A. Reporting Entity

Defense Information Systems Agency (DISA), a combat support agency within the Department of Defense (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), Joint Service Committee (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 Agency Financial Report (AFR) provides a list of the components, which compose 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 Chief Information Officer (CIO) capability planning guidance.

In accordance with SFFAS 47, DISA Working Capital Fund (WCF) does not have any consolidation, related parties or disclosure entities that are required to be disclosed within these notes. Although component reporting entities of the federal government may significantly influence each other, component reporting entities are subject to the overall control of the federal government and operate together to achieve the policies of the federal government and are not considered related parties. Therefore, component reporting entities need not be disclosed as related parties by other component reporting entities. Disclosure entities are not consolidation entities. Disclosure entities may provide the same or similar goods and services that consolidation entities do but are more likely to provide them on a market basis.

1B. Accounting Policies

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

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) [SFFAS 54](#), *Leases: An Amendment of SFFAS 5, Accounting for Liabilities of the Federal Government and SFFAS 6, Accounting for Property, Plant, and Equipment*: Issued April 17, 2018. The requirements of SFFAS 54 were deferred to reporting periods beginning after Sept. 30, 2023 under [SFFAS 58](#), *Deferral of the Effective Date of SFFAS 54, Leases*: Issued June 19, 2020. Early adoption is not permitted. For additional information, see [SFFAS 60](#), *Omnibus Amendments 2021: Leases-Related Topics* [Technical Release 20](#), *Implementation Guidance for Leases*, and [Technical Bulletin 2023-1](#), *Intragovernmental Leasehold Reimbursable Work Agreements*.
- 4) [Technical Bulletin 2020-1](#): *Loss Allowance for Intragovernmental Receivables*. Issued Feb. 20, 2020; Effective upon issuance.

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).

In FY 2024, the Defense Information Systems Agency (DISA) has adopted the reporting guidelines of SFFAS 54, detailing the recognition of right-to-use assets and the corresponding lease liabilities. These reports pertain to non-intragovernmental and non-short-term contracts where DISA retains exclusive rights to specific transoceanic cables that facilitate network and telecommunication services acquired through communication service authorizations (CSAs) within the optical transport network.

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 reporting 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

Section 406 -Intra-Governmental Capitalized Assets Procedures, of the quarterly reporting guidance was updated for fourth quarter of FY 2023 to require agencies to record all direct cost to an expense series account and then offset those amounts using USSGL 6610 when the costs are capitalized to the appropriate asset account. Per this updated guidance, the DISA WCF will no longer record federal USSGL 8802. This update was designed to avoid

a systemic cost of goods sold (USSGL 6500) entry for the selling agency, which does not typically recognize inventory. This process change does not affect prior financial statements, only reconciles interagency expenses and revenues for fourth quarter of FY 2023 and forward.

Starting in FY 2024, Federal reporting entities are required to report a right-to-use asset and a lease liability for non-intragovernmental, non-short-term contracts or agreements, when the entity has the right to obtain and control access to economic benefits or services from an underlying property, plant, or equipment asset for a period of time in exchange for consideration under the terms of the contract or agreement.

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 \$581 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 \$4.4 billion represents funds obligated for goods and services but not paid.

The Non-FBWT budgetary accounts in the amount of \$4.6 billion reduce budgetary resources and are primarily composed of unfilled customer orders without advance from customers in the amount of \$3.6 billion, contract authority in the amount of \$198.6 million, and receivables and other in the amount of \$862.1 million.

Contract 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 24-Fund Balance with Treasury

(thousands)

DISA WCF	<u>2024</u>	<u>2023</u>
1. Unobligated Balance:		
A. Available	\$ 581,001	\$ 370,566
B. Unavailable	29,759	-
Total Unobligated Balance	\$ 610,760	\$ 370,566
2. Obligated Balance not yet Disbursed	\$ 4,444,271	\$ 1,659,920
4. Non-FBWT Budgetary Accounts:		
B. Unfilled Customer Orders without Advance	(3,563,140)	(871,605)
C. Contract Authority	(198,601)	(174,314)
E. Receivables and Other	(862,092)	(679,424)
Total Non-FBWT Budgetary Accounts	\$ (4,623,833)	\$ (1,725,343)
Total FBWT	\$ 431,198	\$ 305,143

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 25-Accounts Receivable, Net

(thousands)

DISA WCF 2024	Gross Amount Due	Allowance for Estimated Uncollectibles	Accounts Receivable, Net
1. Intragovernmental Receivables	\$ 861,571	\$ (3,260)	\$ 858,311
2. Non-Federal Receivables (From the Public)	2,617	(1,038)	1,579
3. Total Accounts Receivable	\$ 864,188	\$ (4,298)	\$ 859,890

DISA WCF 2023	Gross Amount Due	Allowance for Estimated Uncollectibles	Accounts Receivable, Net
1. Intragovernmental Receivables	\$ 875,711	\$ (2,737)	\$ 872,973
2. Non-Federal Receivables (From the Public)	892	(17)	875
3. Total Accounts Receivable	\$ 876,603	\$ (2,754)	\$ 873,848

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

DISA WCF general Property, Plant, and Equipment (PP&E) is composed of telecommunications and computing services with related equipment, software, construction-in-progress, and right-to-use lease assets with a net book value (NBV) of \$1.5 billion.

DISA WCF PP&E consists of telecommunications equipment, computer equipment, computer software, right-to-use lease assets, and construction in progress, whereby the acquisition cost falls within prescribed thresholds and the estimated useful life is two or more years. 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. Per SFFAS 54, right-to-use asset thresholds are left up to the discretion of the agency. DISA hasn't established a right-to-use threshold for FY 2024.

Starting in FY 2024, Federal reporting entities are required to report a right-to-use asset and a lease liability for non-intragovernmental, no-short-term contracts or agreements, when the entity has the right to obtain and control access to economic benefits or services from an asset under the terms of the contract or agreement.

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 26-General Property, Plant, and Equipment, Net
(thousands)

DISA WCF	2024	2023
General PP&E, Net beginning of year	\$ 1,011,566	\$ 1,015,572
Effects of implementation of SFFAS 54	-	-
Balance beginning of year, adjusted	1,011,566	1,015,572
Capitalized Acquisitions	148,854	159,982
Right-to-Use assets, CY activity	614,103	-
CY Amortization of right-to-use assets	(142,047)	-
Dispositions	(9,602)	(11,513)
Transfers in/(out) without reimbursement	96,253	109,457
Depreciation Expense	(232,150)	(261,933)
Balance at end of year	\$ 1,486,977	\$ 1,011,565

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 27-Major General PP&E Asset Classes

DISA WCF 2024 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
Software	S/L	2-5 or 10	\$ 234,947	\$ (182,155)	\$ 52,792
General Equipment	S/L	Various*	2,642,568	(1,852,677)	789,891
Assets Under Capital Lease	S/L	Lease term	-	-	-
Right-to-Use Lease Asset	S/L	Lease term	969,586	(409,374)	560,212
Construction-in-Progress	N/A	N/A	84,082	N/A	84,082
Total General PP&E			\$ 3,931,183	\$ (2,444,206)	\$ 1,486,977

DISA WCF 2023 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
Software	S/L	2-5 or 10	\$ 220,751	(163,639)	\$ 57,111
General Equipment	S/L	Various*	2,586,637	(1,768,758)	817,879
Assets Under Capital Lease	S/L	Lease term	332,784	(270,665)	62,118
Right-to-Use Lease Asset	S/L	Lease term	-	-	-
Construction-in-Progress	N/A	N/A	74,457	N/A	74,457
Total General PP&E			\$ 3,214,629	\$ (2,203,063)	\$ 1,011,565

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

*PE55 and PE56 use 5 years for depreciation and PE54 uses 3 years for most depreciation, unless otherwise specified (10/20 years). DISA follows the FMR Vol. 4 Ch. 25 Table 25-2 for useful life unless specifically stated in contract documents.

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 is composed of DISA WCF's unfunded Federal Employees' Compensation Act (FECA) liability in the amount of \$934.7 thousand. These liabilities will be funded in future periods.

Other than intragovernmental liabilities-federal employee benefits payable consists of various employee actuarial liabilities not due and payable during the current fiscal year. As of Sept. 30, 2024, DISA WCF's liabilities consist of federal employee and veteran benefits payable in the amount of \$4.7 million and Other Liabilities in the amount of \$500 million. Other liabilities consist of unfunded lease liability. These liabilities will be funded in future periods.

Starting in FY 2024, Federal agencies are required to report a right-to-use asset and a corresponding lease liability for material non-intragovernmental, no-short-term contracts when the reporting entity has the right to control access to and obtain benefits from the use of real property, equipment, or other PP&E.

Figure 28-Liabilities Not Covered by Budgetary Resources

(thousands)

DISA WCF	<u>2024</u>	<u>2023</u>
Intragovernmental Liabilities		
Other	\$ 935	\$ 853
Total Intragovernmental Liabilities	935	853
Other than Intragovernmental Liabilities		
Federal employee and veteran benefits payable	4,701	4,941
Other Liabilities	499,976	-
Total Other than Intragovernmental Liabilities	504,677	4,941
Total Liabilities Not Covered by Budgetary Resources	505,612	5,794
Total Liabilities Covered by Budgetary Resources	924,261	1,002,692
Total Liabilities	\$ 1,429,873	\$ 1,008,486

Note 6. Current and Former Federal Employee and Veterans Benefits Payable

Expense Components

For FY 2024, 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 \$8.9 million in total, of which \$4.7 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.

SFFAS 5, Accounting for liabilities of the federal government is not applicable to DISA since they are not an administrative entity.

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 \$239.3 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 29-Current and Former Federal Employee and Veterans Benefits Payable
(thousands)

DISA WCF 2024	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
Other Benefits			
FECA	\$ 4,701	\$ -	\$ 4,701
Other-Salary Related	52,298	(52,298)	-
Total Other Benefits	56,999	(52,298)	4,701
Federal Employee Benefits Payable	56,999	(52,298)	4,701
Other benefit-related payables included in Intragovernmental Other Liabilities	3,373	(2,438)	935
Total Federal Employee Benefits Payable	\$ 60,372	\$ (54,736)	\$ 5,636

DISA WCF 2023	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
Other Benefits			
FECA	\$ 4,941	\$ -	\$ 4,941
Other-Salary Related	47,423	(47,423)	-
Total Other Benefits	52,364	(47,423)	4,941
Federal Employee Benefits Payable	52,364	(47,423)	4,941
Other benefit-related payables included in Intragovernmental Other Liabilities	2,737	(1,884)	853
Total Federal Employee Benefits Payable	\$ 55,101	\$ (49,307)	\$ 5,794

Note 7. Other Liabilities

Intragovernmental

Federal Employee and Veteran Benefits Payable: \$2.8 million. This represents liabilities for administering pensions, Other Retirement Benefits (ORB), and Other post-employment benefits (OPEB) (including post-retirement health, life insurance, veterans' compensation and burial, and veteran education benefits).

Other Than Intragovernmental

Accrued funded payroll and benefits: 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.

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 30-Other Liabilities

(thousands)

DISA WCF 2024	Current Liability	Non-Current Liability	Total
Intragovernmental			
Liabilities for Non-entity Assets	\$ -	\$ -	\$ -
Subtotal	-	-	-
Other Liabilities	2,772	601	3,373
Total Intragovernmental	2,772	601	3,373
Other than Intragovernmental			
Right-to-use lease liability	-	499,976	499,976
Total Other than Intragovernmental	-	499,976	499,976
Total Other Liabilities	\$ 2,772	\$ 500,577	\$ 503,349
DISA WCF 2023			
	Current Liability	Non-Current Liability	Total
Intragovernmental			
Liabilities for Non-entity Assets	\$ 2	\$ -	\$ 2
Subtotal	2	-	2
Other Liabilities	2,251	486	2,737
Total Intragovernmental	2,252	486	2,738
Other than Intragovernmental			
Accrued Funded Payroll and Benefits	-	-	-
Total Other than Intragovernmental	-	-	-
Total Other Liabilities	\$ 2,252	\$ 486	\$ 2,738

Note 8. Leases

In FY 2024, DISA has adopted the reporting guidelines of SFFAS 54, detailing the recognition of right-to-use assets and the corresponding lease liabilities. These guidelines pertain to non-intragovernmental, long-term contracts (greater than 24 months) where DISA retains exclusive rights to specific transoceanic cables that facilitate network and telecommunication services acquired through communication service authorizations (CSAs) within the optical transport network. WCF is the lessee in these agreements, obtaining the right to control the use of asset, rather than granting control (as the lessor would).

According to SFFAS 54, a lease is characterized as a contractual arrangement in which one party (the lessor) grants another party the right to control the use of property, plant, and equipment (PP&E), identified as the underlying asset. Within the context of CSA contracts, the services may encompass circuit connectivity, often utilizing a physical component known as a "trunk." These trunks, which form the basis of the circuit connection, are considered the underlying assets essential for lease accounting. DISA WCF acquires and manages commercial telecommunication leases on behalf of the federal government. DISA WCF is a lessor for the sub-lease telecommunications for other federal agencies.

DISA has elected to execute the embedded lease accommodation through Sept. 30, 2026, in accordance with paragraph 96A-96E of SFFAS-54.

As of Sept. 30, 2024, DISA is recognizing a total of 3,430 right-to-use assets, which include telecommunication, commercial space, office equipment and fiber optic cables. These leasing arrangements have terms from 2 to 12 years.

Land and Building Leases

As of Sept. 30, 2024, DISA WCF operates in 18 locations, of which 17 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 intragovernmental. This lease generally requires DISA WCF to pay property taxes, utilities, security, custodial services, parking, and operating expenses. Certain leases contain renewal options. Annual lease expense for the building lease in FY 2024 is \$731.7 thousand.

In addition, DISA WCF currently has four non-federal, long-term lease arrangements each with a five-year lease term. These include two warehouse leases; one agreement for two data centers (located in Miami, FL, and Culpeper, VA); and one ground facility agreement supporting bandwidth services.

Equipment Leases

DISA WCF currently leases 131 photocopiers within two agreements and 20 vehicles within one agreement located across various sites. The photocopiers are leased for three years, while the vehicles are leased for one year with an annual renewal option. Annual lease expense for the equipment leases in FY 2024 is \$455 thousand.

DISA WCF currently has one non-federal, long-term lease arrangement for a multifunction printer that is being leased for three years.

The following table provides the current right-to-use asset cost and accumulated amortization as of Sept. 30, 2024, for leases other than (1) short-term leases, (2) contracts or agreements that transfer ownership, and (3) intragovernmental agreements:

Figure 31-Right-to-Use Asset Net Book Value

(thousands)		
RTUA	Accumulated Amortization	Net Book Value (RTUA – A/A)
\$636,803	\$ 130,259	\$ 506,544

The following table provides future lease payments, as of Sept. 30, 2024, for leases other than (1) short-term leases, (2) contracts or agreements that transfer ownership, and (3) intragovernmental agreements:

Figure 32-Future Payments Right-to-Use Leases

(thousands)

DISA WCF 2024				
<u>Principal</u>				
	Land and Buildings	Equipment	Other	Total
Fiscal Year				
2025	\$ 3,496	\$ 44	\$ 140,965	\$ 144,505
2026	3,593	4	118,502	122,099
2027	2,972	-	67,199	70,171
2028	2,016	-	56,195	58,211
2029	824	-	31,045	31,869
2030 - 2034	-	-	73,583	73,583
	<u>\$ 12,901</u>	<u>\$ 48</u>	<u>\$ 487,489</u>	<u>\$ 500,438</u>

<u>Interest</u>				
	Land and Buildings	Equipment	Other	Total
Fiscal Year				
2025	\$ 523	\$ 1	\$ 19,013	\$ 19,537
2026	359	-	12,696	13,055
2027	197	-	8,516	8,713
2028	87	-	5,845	5,932
2029	17	-	3,880	3,897
2030 - 2034	-	-	4,352	4,352
	<u>\$ 1,183</u>	<u>\$ 1</u>	<u>\$ 54,302</u>	<u>\$ 55,486</u>

<u>Total</u>				
	Land and Buildings	Equipment	Other	Total
Fiscal Year				
2025	\$ 4,019	\$ 45	\$ 159,978	\$ 164,042
2026	3,952	4	131,198	135,154
2027	3,169	-	75,715	78,884
2028	2,103	-	62,040	64,143
2029	841	-	34,925	35,766
2030 - 2034	-	-	77,935	77,935
	<u>\$ 14,084</u>	<u>\$ 49</u>	<u>\$ 541,791</u>	<u>\$ 555,924</u>

The following is a summary of the range of interest rates used to calculate the lease liability. These are based on marketable Treasury securities of similar maturity to the term of the lease. Interest rates are rounded down to the nearest maturity:

Figure 33-Interest Rate Range

Term in Years	Interest rate range
2	3.5% - 5%
3-4	3.375% - 4.625%
5-6	3.5% - 4.875%
7-9	3.625% - 4.875%
10	3.875% - 4.5%

DISA WCF currently has 3,881 (1,168 short-term and 2,713 long-term) intragovernmental lessor arrangements. Below is a table of future lease payments that are to be received from other federal agencies:

Figure 34-Future Payments Intragovernmental Leases
(thousands)

DISA WCF 2024	Asset Category			
	Land and Buildings	Equipment	Other	Total
1. Federal				
Fiscal Year				
2025	\$ 1,108	\$ 45	\$ 61,703	\$ 62,856
2026	1,002	4	38,975	39,981
2027	924	-	28,605	29,529
2028	970	-	23,813	24,783
2029	842	-	19,952	20,794
2030 - 2034	-	-	39,803	39,803
Total Intragovernmental Future Lease Payments	<u>\$ 4,846</u>	<u>\$ 49</u>	<u>\$212,851</u>	<u>\$217,746</u>

DISA WCF does not currently have any non-federal lessor arrangements. WCF can only be a lessor for intragovernmental leasing arrangements.

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 2024 reporting.

Note 10. 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 11. 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, 2024, DISA WCF incurred \$9.3 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, 2024, is \$581 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, 2024, DISA WCF's net amount of budgetary resources obligated for undelivered orders is \$3.5 billion.

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

(thousands)

DISA WCF	2024	2023
Intragovernmental		
Unpaid	\$ 151,891	\$ 38,109
Total Intragovernmental	<u>151,891</u>	<u>38,109</u>
Non-Federal		
Unpaid	3,370,121	815,401
Prepaid/Advanced	2,000	-
Total Non-Federal	<u>3,372,121</u>	<u>815,401</u>
Total Budgetary Resources Obligated for Undelivered Orders at the End of the Period	<u>\$ 3,524,012</u>	<u>\$ 853,510</u>

Note 12. 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 36- Reconciliation of the Net Cost of Operations to Net Outlays

(thousands)

DISA WCF 2024	Intragovernmental	With the Public	Total
Net Cost (Revenue) reported on SNC	\$ (8,490,050)	\$ 8,463,304	\$ (26,746)
Components of Net Cost Not Part of Net Outlays:			
Property, plant, and equipment depreciation expense	-	(232,150)	(232,150)
Property, plant, and equipment disposals & revaluations	-	86,651	86,651
Lessee Lease Amortization	-	(142,047)	(142,047)
Property, plant, and equipment		14,322	14,322
Increase/(Decrease) in Assets:			
Accounts receivable, net	(14,662)	704	(13,958)
Advances and Prepayments	-	2,000	2,000
(Increase)/decrease in liabilities:			
Accounts Payable	8,423	77,436	85,859
	-	114,127	114,127
Federal employee salary, leave, and benefits payable	-	(4,875)	(4,875)
	-	239	239
Advances from Others and Deferred Revenue	(2,000)	-	(2,000)
Other liabilities	(636)	-	(636)
Other Financing Sources:			
Imputed cost	(45,123)	-	(45,123)
Total Components of Net Cost That Are Not Part of Net Outlays	(53,998)	(83,594)	(137,592)
Components of Net Outlays That Are Not Part of Net Cost:			
Acquisition of Capital Assets	-	134,532	134,532
Financing Sources			
Transfers (in)/out without reimbursements	(96,252)	-	(96,252)
Total Components of Net Budgetary Outlays Not Part of Net Cost	(96,252)	134,532	38,280
Total Other Reconciling items	-	-	-
Total Net Outlays	\$ (8,640,300)	\$ 8,514,242	\$ (126,058)
Agency Outlays, Net, Statement of Budgetary Resources			\$ (126,056)
Unreconciled difference			\$ (2)

Note 13. Disclosure Entities and Related Parties

Pursuant to SFFAS 47 reporting disclosure requirements, related parties are considered related if: (1) one party to an established relationship, has the ability to exercise significant influence over the other party in making policy decisions and (2) the relationship is of such significance that it would be misleading to exclude information about it. After review of SFFAS 47, appendix B and the associated criteria, it was determined DISA does not have consolidated entities, disclosure entities nor related parties.

**Defense Information Systems Agency
Working Capital Fund
Required Supplementary Information
Fiscal Year 2024, Ending Sept. 30, 2024**

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 2024 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, it poses 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 2024, all real property has been transferred out of the DISA WCF.

For FY 2024, 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.

For FY 2024, significant entities are encouraged (and for FY 2025, significant entities will be required) to: (1) describe their method for estimating deferred maintenance and repairs and how inflation in labor and materials costs is used to annually adjust the estimates and (2) report the minimum maintenance and repair amount needed to ensure that mission critical facilities remain mission capable. Maintenance and repairs are based on manufacturers life cycle replacement criteria. Also building condition assessments are conducted to capture all systems, components, and sub-components. The assessments provide greater detail to forecast and budget for these repairs in the outyears. Funding is requested in the POM. There are limited funds even though forecasting has identified repair projects. Have not designated a minimum maintenance or repair amount at each facility. An annual facility data call is issued to the organizations. Repair/Sustainment projects are prioritized: life safety, mission critical and repairs. Mission critical facilities have not been impacted by deferred maintenance. These facilities remain mission capable. Projects which are deferred to the following year – project costs have an escalation factor 2.1%.

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
Other Information
Fiscal Year 2024, Ending Sept. 30, 2024**

Summary of Financial Statement Audit and Management Assurances

Audit Opinion: Unmodified

Restatement: No

Figure 37-Summary of Financial Statement Audit

Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Ending Balance
Fund Balance with Treasury	3	0	3	0	0
Total Material Weaknesses	3	0	3	0	0

Figure 38- Summary of Management Assurances

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	3	0	3	0	0	0
Accounts Payable/Expense	0	0	0	0	0	0
Accounts Receivable/Revenue	0	0	0	0	0	0
Internal Controls	0	0	0	0	0	0
Unmatched Transactions	0	0	0	0	0	0
Financial Reporting	0	0	0	0	0	0
Undelivered Orders	0	0	0	0	0	0
Unfilled Customer Orders	0	0	0	0	0	0
PPE	0	0	0	0	0	0
Total Material Weaknesses	3	0	3	0	0	0

Effectiveness of Internal Control over Operations (FMFIA§ 2)

Statement of Assurance: Unmodified

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

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	0	0	0	0	0	0
Total non-conformance	0	0	0	0	0	0

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	No lack of compliance noted
Applicable Federal Accounting Standards	No lack of compliance noted	No lack of compliance noted
USSGL at Transaction Level	No lack of compliance noted	No lack of compliance noted

Management Challenges



DEFENSE INFORMATION SYSTEMS AGENCY

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

24 October 2024

SUBJECT: Top Management and Performance Challenges Facing the Defense Information Systems Agency (DISA) in Fiscal Year 2025

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 2025.

In developing this report, the DISA OIG considered several criteria including items such as the impact on safety and cyber security, documented vulnerabilities, large dollar implications, high risk areas, and the ability of DISA to effect change. We reviewed recent and prior internal audits, evaluations, and investigation reports; reports published by other oversight bodies; and input received from DISA senior leadership.

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 2025 include:

- Meeting Data Management Challenges
- Managing Human Capital
- Mission Partner Payments
- Property Management and Accountability
- Artificial Intelligence

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

Within the Department of Defense (DoD), data management is the execution of directives to acquire, control, protect, and enhance the value of data assets. As a combat support agency (CSA), DISA implements and sustains global transport, voice, video, and data for mission partners while maintaining various operating systems that produce large and complex datasets. The federal government, 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 hostile state-sponsored hackers targeted and breached U.S. defense and industry critical infrastructure in the past.

DISA is responsible for helping the DoD modernize the infrastructure and identify, protect, detect, respond, and recover from data threats within DISA's area of operations. The DISA Office of the Chief Data Officer (OCDO) was formally established in September 2021. In 2022, the Chief Data Officer (CDO) published the DISA Data Strategy Implementation Plan v1.0 (IPlan v1.0), describing a modern approach to information architecture and data management and outlining workstreams necessary to organize activities, define activities, and identify next steps for the DISA organization, covering the years for FY2022-FY2024. The DISA IPlan v1.0 aligned with the 2020 DoD Data Strategy, DISA Strategic Plan FY2022-2024, and expanded upon DISA's efforts to meet DoD data management principles, capabilities, and goals by leveraging data as a center of gravity. DISA also created the DISA Data Analytics Center of Excellence to bridge business policies, cyber, and information technology.

To tackle current and future challenges, the DoD outlined specific data management goals in the 2023 Data, Analytics, and Artificial Intelligence Adaptation Strategy. Per the Strategy, DoD aims to protect data and evolve data into actionable information for decision makers. The DoD Strategy describes the DoD vision, guiding principles, essential capabilities, and goals for data management throughout the DoD. To meet the current DoD strategy and DISA's evolving data and AI needs, the CDO will publish a new DISA Data Plan in Q1 FY2025. When published, this new DISA Data Plan, and subsequent IPlan v2.0, will align with the DoD 2023 Data, Analytics, and Artificial Intelligence Adoption Strategy and the DISA Next Strategy.

In 2024, the DISA OIG published an evaluation of DISA's data management maturity. The OIG found DISA's data management was at the beginning of a multi-year process to manage institutional change and adopt a data-centric culture. The OIG had five recommendations to help DISA reach higher levels of maturity. Since the report was published, DISA has updated the DISA Data Catalog Business glossary, created a Data Readiness Assessment (DRA) Scorecard, and implemented and integrated the DRA Scorecard into Chief Engineering Panel (CEP) processes.

Challenge 2

Managing Human Capital

Recruiting individuals with the right talent in a timely manner is critical and continues to be a challenge. DISA competes for talent with the private sector, where additional benefits and flexibilities can be used to recruit highly qualified workers. Whether individuals are recent college graduates, high-performing industry professionals, or military veterans with years of experience in the field, DISA's goal is to make the Agency a place sought out by high-caliber talent.

To address this challenge, DISA continues to strengthen the work culture, invest in key initiatives to attract and retain a talent pool skilled in critical thinking and diverse in ideas, backgrounds, and technical expertise. DISA is also forecasting needed skills through succession planning, improving how DISA markets career opportunities within the agency, and deepening external partnerships with educational institutions and third-party personnel services. DISA's telework and remote work policies also allow leadership to broaden the hiring pool of candidates in various geographical regions to attract and retain high quality talent.

Workforce 2025 is DISA's recent initiative designed to address longstanding cyber workforce challenges, including attracting, training, and promoting a workforce that is equipped with the knowledge and decision-making abilities to "creatively solve national security challenges in a complex global environment." DISA released *Workforce 2025 Implementation Plan* in September 2023, and the Plan is a living document that may change due to resources and/or strategic and workforce priorities.

The *Workforce 2025* strategy is designed to enhance the skills and talents of current employees while ensuring DISA onboards new talent and invests in the professional development of both throughout their careers. *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. *Workforce 2025* will establish a culture enabling the Agency to rapidly adapt to inevitable technological advances and mission portfolio adjustments ensuring DISA delivers relevant, cutting-edge capabilities so our Warfighters gain and maintain an operational and competitive edge.

In 2024, the DISA OIG published an evaluation of DISA's hiring process. Overall, the OIG found inefficiencies across the hiring process and staff could not effectively track hiring actions because of insufficient hiring guidance, training, platforms, metrics, and accountability. To address these challenges, the OIG recommended DISA improve training and create a detailed guidebook that includes authorities, responsibilities, and process timelines. The OIG also recommended DISA develop a platform to track hiring from the time a position is vacant to the first day of employment.

Challenge 3

Mission Partner Payments

Accurate, auditable reporting of financial and budgeting information allows DISA to obtain optimal resources to ensure mission success. DISA operates with two funding types: General Fund (GF) and Working Capital Fund (WCF). DISA has a total budget of \$11.9 billion and receives funding through both congressional appropriations of \$3.4 billion and WCF of \$8.5 billion.

In FY 2023, DISA's GF financial statements received a disclaimer of opinion because DISA was unable to provide sufficient evidence for the independent auditor to produce an opinion and the independent auditors found material weaknesses. DISA's WCF financial statements received an unmodified opinion.

DISA, like other service providers in the Department of Defense, experiences delinquent accounts receivable as part of doing business with various mission partners. DISA continues to have challenges obtaining Mission Partner (Military Services and Defense/Non-Defense Agencies) funding in a timely manner for reimbursable costs incurred.

In FY 2023, the DISA Office of the Inspector General (OIG) conducted an audit of DISA's Reimbursable Services Collections to determine whether DISA collects accounts receivables for reimbursable services in accordance with DoD and DISA guidance. DISA OIG made six recommendations and two of six recommendations have been implemented, resulting in decreased uncollected aged accounts receivables. Incomplete and limited automated capabilities to accomplish and carryout financial activities for the collection process hinders DISA's ability to receive timely reimbursement for services provided.

DISA is planning to standardize customer engagement and delinquent customer notices across the GF and WCF to build a more consistent and streamlined process preventing aged accounts receivable bills from occurring. The updated policy, once signed, will identify and enforce a standard process across DISA.

DISA must remain diligent in their efforts to develop and implement corrective action plans for identified findings and recommendations to improve the production of reliable financial information and ensure a competitive advantage for the warfighter on the battlefield.

Challenge 4

Property Management and Accountability

Property management and accountability is a top management challenge for DISA. For FY 2023, Property, Plant, and Equipment reported on DISA's balance sheets included General Fund (GF) \$325 million and Working Capital Fund (WCF) \$1 billion. In FY 2023, DISA's WCF Annual Financial Report included a repeat significant deficiency pertaining to a lack of accountability over Property, Plant, and Equipment.

Property management includes the functions of determining property requirements, receipt, storage, distribution, utilization, and disposal of property. Property management and accountability is a challenge across DoD. The DISA OIG has conducted several property audits and reported concerns relating to property management and accountability at DISA; specifically, concerns included: decentralized program property management functions, overarching policies and procedures, warehouse property management, proper oversight, property obsolescence, backlogs of property awaiting final disposal, Government Furnished Property in the possession of contractors, accountability of mobile device, etc. These audit findings illustrate the challenges facing DISA when managing and accounting for property. The DISA OIG has made several recommendations to help improve the internal controls for property accountability.

DISA continues to work to improve oversight of accountable property. DISA's J4 is creating overarching guidance for property management and accountability to improve internal controls.

Challenge 5

Artificial Intelligence

Artificial intelligence (AI) refers to the ability of machines to perform tasks that normally require human intelligence. For example, AI includes recognizing patterns, learning from experience, drawing conclusions, making predictions, or acting. Examples of AI enabled technology include chatbots that facilitate writing, tools for intelligence analysis, and autonomous weapon systems. Strategic competitors, such as China and Russia, are also making significant investments in AI.

AI will transform warfare, and failure to adopt AI technology could hinder national security. According to the DISA Director, generative AI is “probably one of the most disruptive technologies and initiatives in a very long, long time. Those who harness that and can understand how to best leverage it, but also how to best protect against it, are going to be the ones that have the high ground.”

In response to this challenge, the 2018 DoD AI Strategy directs the DoD to accelerate the adoption of AI and the creation of a force that can protect the security of our nation. In 2022, DoD also published a Responsible AI (RAI) Strategy and Implementation pathway that illuminates the path forward by defining and communicating a framework for harnessing AI.

DISA is also looking for ways to repurpose cutting-edge technology like AI for cyber analytics, cyber protection, and operations to protect the Defense Department's global network. For example, DISA held an AI Summit for participants to learn about various AI initiatives within DISA and around the DoD. Participants had the opportunity to meet leaders that specialize in AI and observed demonstrations by the Joint Artificial Intelligence Center, DISA, and Industry Leaders. DISA also issued Initial Guidance on the Responsible Use of Publicly Available Generative Artificial Intelligence Tools.

While DISA is moving forward in the pursuit of integrating the use of AI into DISA’s mission to protect the Defense Department’s global network, there is an increased challenge of ensuring that government-related materials, both Classified and Controlled Unclassified Information (such as Personal Identifiable Information (PII)) is protected from being uploaded into publicly available Generative AI tools. Even though the use of available AI tools for appropriate cases will be encouraged, DoD personnel must do so safely and responsibly and adhere to the responsible acquisition, deployment, and use of AI through established policies, including DoD’s AI Ethical Principles.

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. 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 ensuring external agency objectives are met while minimizing the impact to DISA operations. OIG Liaison supports DISA as a whole by providing:

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

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 2024.

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



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

November 8, 2024

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 2024 and FY 2023
(Project No. D2024-D000FL-0067.000, Report No. DODIG-2025-028)

We contracted with the independent public accounting firm of Kearney & Company, P.C. (Kearney) 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, 2024, and 2023. The contract required Kearney 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 Working Capital Fund's financial management systems substantially complied with the requirements of the Federal Financial Management Improvement Act of 1996. The contract required Kearney 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," Volume 1, June 2024; Volume 2, June 2024; and Volume 3, July 2024. Kearney's Independent Auditor's Reports are attached.

Kearney's audit resulted in an unmodified opinion. Kearney concluded that the DISA Working Capital Fund Financial Statements and related notes as of and for the fiscal years ended September 30, 2024, and 2023, were presented fairly, in all material respects, and in accordance with Generally Accepted Accounting Principles.

Kearney's separate report, "Independent Auditor's Report on Internal Control Over Financial Reporting," did not identify any material weaknesses related to the DISA

Working Capital Fund's internal controls over financial reporting.* Kearney's additional report, "Independent Auditor's Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements," did not identify any instances of noncompliance with provisions of applicable laws and regulations, contracts, and grant agreements.

In connection with the contract, we reviewed Kearney's reports and related documentation and discussed them with Kearney'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 2024 and FY 2023 Financial Statements and related notes. Furthermore, we do not express conclusions on the effectiveness of internal controls over financial reporting, on whether the DISA Working Capital Fund'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 did not comply, in all material respects, with GAGAS. Kearney is responsible for the attached November 8, 2024 reports and the conclusions expressed within the reports.

We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me.

FOR THE INSPECTOR GENERAL:



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

Attachments:

As stated

* 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.

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 financial statements of the Defense Information Systems Agency (DISA) Working Capital Fund (WCF), which comprise the Balance Sheets as of September 30, 2024 and 2023, 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, 2024 and 2023 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. 24-02, *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.

Emphasis of Matter

As discussed in Note 1 to the financial statements, in fiscal year 2024, DISA WCF adopted new accounting guidance issued by the Federal Accounting Standards Advisory Board (FASAB), specifically Statement of Federal Financial Accounting Standards (SFFAS) No. 54, *Leases*, and SFFAS No. 62, *Transitional Amendment to SFFAS 54*. Additional information on DISA WCF's leases is provided in Notes 4, 5, and 8. Our opinion is not modified with respect to this matter.

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 a reasonable period of time 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 GAAS and *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 GAAS and *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 beyond the financial statement date.

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 Management's Discussion and Analysis, Deferred Maintenance and Repairs, and Combining Statement of Budgetary Resources be presented to supplement the financial statements. Such information is the responsibility of management and, although not a part of the financial statements, is required by OMB and FASAB, who consider it to be an essential part of financial reporting for placing the financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the RSI in accordance with GAAS, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the financial statements, and other knowledge we obtained during our audits of the 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 Management Assurances, Management Challenges, and Payment Integrity sections 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. 24-02, we have also issued reports, dated November 8, 2024, on our consideration of DISA WCF's internal control over financial reporting and on our tests of DISA WCF's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements, as well as other matters for the year ended September 30, 2024. 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. 24-02 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
November 8, 2024

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. 24-02, *Audit Requirements for Federal Financial Statements*, the financial statements, and the related notes to the financial statements of the Defense Information Systems Agency (DISA) Working Capital Fund (WCF) as of and for the year ended September 30, 2024, which collectively comprise DISA WCF's financial statements, and we have issued our report thereon dated November 8, 2024.

Report on 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. 24-02. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations.

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. 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.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section 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. Given these limitations, during our audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses.



We did identify certain deficiencies in internal control, as described in the accompanying **Schedule of Findings** as Items I, II, and III that we consider to be significant deficiencies.

During the audit, we noted certain additional matters involving internal control over financial reporting that we will report to DISA WCF's management in a separate letter.

The Defense Information Systems Agency Working Capital Fund'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. 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 and, 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. 24-02 in considering DISA WCF's internal control. Accordingly, this report 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
November 8, 2024

Schedule of Findings

Significant Deficiencies

Throughout the course of our audit work at the Defense Information Systems Agency (DISA) Working Capital Fund (WCF), 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 1* presents the significant deficiencies identified during our audit.

Exhibit 1: Significant Deficiencies and Sub-Categories

Significant Deficiency	Significant Deficiency Sub-Categories
I. Fund Balance with Treasury	A. Suspense Reconciliation and Reporting Process B. Statement of Differences Reconciliation and Reporting Process
II. Property, Plant, and Equipment	A. Untimely Asset Activation
III. Information Technology	A. Defense Information Systems Agency Risk Management Framework B. Financial Accounting Management Information System – Working Capital Fund Database Audit Logging and Monitoring C. Incomplete Financial Accounting and Budget System Application Access Request Documentation D. Incomplete Complementary User Entity Controls Implementation

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

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

- A. Suspense Reconciliation and Reporting Process
- B. Statement of Differences Reconciliation and Reporting Process

A. Suspense Reconciliation and Reporting Process

Background: DISA WCF’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). In addition to monitoring and approving the FBWT reconciliations performed by its service organization on its behalf, DISA WCF is responsible for the complete and accurate reporting of FBWT on its financial statements and disclosures.

Suspense 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 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 suspense accounts are available for obligation or expenditure while in suspense. Agencies should have a process to research and properly record suspense account transactions in their general ledgers (GL) timely. Transactions recorded in DoD suspense are required to be reconciled monthly and moved to the appropriate Line of Accounting (LOA) within 60 business days from the date of transaction.

On behalf of DoD agencies, including DISA WCF, DISA WCF's service organization prepares materiality assessments quarterly using a combination of historical data and the current quarter's raw Universe of Transactions (UoT) to estimate the potential impact of outstanding suspense transactions to each DoD entity. The raw UoTs have not been fully researched to identify transaction count and dollar amount impact to DISA WCF and other DoD entities and could contain summary lines. Fully researched UoTs are not available until 53 days after quarter-end and year-end financial reporting timelines.

DISA WCF suspense transactions, if any, at the time of initial recording, are not included on DISA WCF's financial statements. This increases the risk of a misstatement on DISA WCF's reported FBWT, as well as the other impacted line items, including Accounts Payable (AP) for disbursements, Accounts Receivable (AR) for collections, and the related budgetary accounts.

DISA WCF must reconcile its FBWT activity monthly per the Treasury Financial Manual (TFM).

Condition: DISA WCF, 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 WCF collections and disbursements that should be recognized in DISA WCF's accounting records. Additionally, DISA WCF does not have effective controls over the validation of its recorded disbursements and collections, as they impact complementary line items, including AP, AR, and related line items on the Statement of Budgetary Resources, to ensure it is accounting for all transactions that should be reported on its books. The processes currently in place cannot be relied upon to prevent, detect, or correct misstatements in time for quarterly and fiscal year (FY)-end financial reporting.

While DISA WCF's service organization prepares quarterly suspense materiality assessments for each Treasury Index (TI) to advise DISA WCF and other Defense agencies of the potential count and dollar amount of suspense transactions belonging to them, based on previously resolved and cleared suspense transactions, the uncleared suspense transactions included in the assessment are material. As of FY 2024 Quarter (Q) 3, the following were noted as "to be determined" (TBD) in the suspense final UoTs:

- TI-17: 170/1,400 transactions (12%) for \$1.9 million net; \$7.5 million absolute (ABS) (43%)
- TI-21: 775/2,703 transactions (29%) for (\$20.8 million) net; \$33.8 million ABS (28%)

- TI-57: 312/953 transactions (33%) for (\$5.3 million) net; \$17 million ABS (48%)
- TI-97: 14,372/15,165 transactions (95%) for (\$61.2 million) net; \$403.9 million ABS (73%).

In addition, DISA WCF's service organization has not implemented effectively operating control activities to ensure the accuracy and completeness of the suspense UoTs. Specifically, of the samples selected from the Q2 suspense UoT for testing, 33 were identified as either requiring on-site testing, summary lines, or both. DISA WCF's service organization did not know the status of these samples until after selection and did not communicate the additional testing efforts required for these samples in a timely manner. These factors created unforeseen challenges and increased risks to DISA WCF's FBWT. The summary lines and other transactions requiring on-site testing increased required testing efforts and provided further evidence of the risk that the suspense population was inaccurate and incomplete. This also created a risk that the samples could not be supported and tested, either due to limitations of on-site testing or the inability of DISA WCF's service organization to provide additional sample documentation timely.

Specifically:

- Five samples were identified as summary lines which extrapolated to a total of 188 individual transactions. Due to the need to select sub-samples, the tested amount for the TI-21 samples increased from \$16.3 million ABS to \$17 million ABS, respectively. The TI-97 sample increase could not be confirmed, as the ABS amounts were not provided in the sub-sample populations
- Twenty-eight samples were identified as requiring on-site testing for (\$38.8 million) net; \$125 million ABS, or 18% of the total sample selection by ABS dollars.

Cause: DISA WCF'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. That manual research and resolution is what supports the production of the final UoTs and materiality assessments but takes a significant amount of time, which is the cause of them not being available in a timely manner for financial reporting. Additionally, at the time of UoT availability, there has been a significant volume of transactions for a material dollar amount in suspense that has not been identified to an entity and is listed in the UoT as "TBD," as well as unknown samples that require on-site testing and summary line transactions.

In addition, DISA WCF and its service organization have not designed and implemented a methodology to determine the financial reporting impact of DoD suspense account balances to DISA WCF's financial statements for financial reporting in a timely manner sufficient for quarterly and annual financial reporting timelines, including the impact of possible missing collections and disbursements for AP and AR. The assessments do not identify amounts attributed to DISA WCF for the current quarter, but estimate the amount based on historical data. Per Statement of Federal Financial Accounting Standards (SFFAS) No. 1, *Accounting for Selected Assets and Liabilities*, DISA WCF's FBWT represents its claim to the Federal Government's resources and its accounts with Treasury for which DISA WCF is authorized to make expenditures and pay liabilities. The materiality assessment methodology is not designed

effectively as it pertains to recording a FBWT projection, should a material misstatement be identified. SFFAS No. 1 does not permit FBWT as a viable account for estimated amounts.

Effect: DISA WCF 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 effective internal controls and processes to determine the financial reporting impact of the suspense balances inhibits DISA WCF's ability to assert to the completeness and accuracy of reported FBWT on its Balance Sheet and other related financial statement line items, as applicable.

Recommendation: Kearney & Company, P.C. recommends that DISA WCF perform the following:

1. Coordinate with its service organization to continue to develop procedures to determine what portion of the suspense balances, if any, should be attributed to DISA WCF for financial reporting in a timely manner and made available for year-end financial reporting purposes.
2. Coordinate with its service organization to continue to monitor and track the resolution of suspense activity cleared to DISA WCF to enable the entity to perform root cause analysis. This includes further research and resolution over the transactions not resolved in the UoTs and listed as "TBD."
3. Coordinate with its service organization to 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. Coordinate with its service organization to continue to develop and implement processes and controls to eliminate instances where transactions are being placed in suspense accounts intentionally.
5. Coordinate with its service organization to continue to develop and implement a process to establish unique identifiers for each transaction in suspense UoTs that roll forward from period to period. DISA WCF's service organization should develop controls over the establishment and roll-over of those unique identifiers that can be tested for reliance.
6. Coordinate with its service organization to develop and implement a process to validate that all lines in a UoT that are considered "final" are detail lines and not summary lines.
7. Continue implementing business process improvements in the related financial statement line items to prevent items from reaching suspense. Specifically, DISA WCF should develop and implement monitoring controls and processes for AR and AP balances to reduce the risk of DISA WCF having a material amount of disbursements and collections not reflected on its financial statements.
8. Research and resolve suspense transactions by correcting the transactions in source systems and assist DISA WCF's service organization with necessary supporting documentation for corrections, if needed.
9. Obtain and review the quarterly materiality assessments and underlying transaction data to identify root causes of why DISA WCF's transactions are in suspense and not on DISA WCF's books. DISA WCF should design and implement processes and controls to respond to those root causes.

10. Pursuant to receiving the necessary information and documentation from DISA WCF's service organization, develop and implement procedures to identify DISA WCF's suspense account balances for recording and reporting into the GLs and financial statements.

B. Statement of Differences Reconciliation and Reporting Process

Background: DISA WCF'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 WCF'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.

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 by Treasury each month in the Central Accounting Reporting System (CARS). The SOD report identifies discrepancies between the collections and disbursements reported to Treasury and the transactions that were processed by the ALCs each month (i.e., the month the report is generated).

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 within the ALCs are required to research and resolve DIT, IPAC, and Check Issued differences monthly. DISA WCF's service organization has three reporting ALCs which are responsible for month-end reporting of collections and disbursements to Treasury. Further, as a reporting entity, DISA WCF is responsible for monitoring differences identified on the FMS 6652 for the ALCs that process its transactions to determine whether its transactions are included in an SOD and erroneously omitted from its financial statements.

DISA WCF must reconcile its FBWT activity monthly per the TFM.

Condition: DISA, in coordination with its service organization, has not implemented a monitoring control to ensure that transactions that compose the SOD balances in DISA's primary DSSNs do not contain DISA collections and disbursements that should be recognized in DISA's accounting records. The processes currently in place cannot be relied upon to prevent, detect, or correct misstatements in time for quarterly and FY-end financial reporting. While DISA's service organization prepares quarterly SOD materiality assessments at the DSSN level, for DISA's service organization-managed DSSNs, to identify the total count and dollar value of the SOD transactions resolved to DISA and other Defense agencies, the uncleared SOD transactions included in the assessments are significant.

Cause: DISA WCF's service organization's process to create the UoT for SODs is a time-intensive and manual process that requires the consolidation of multiple files from various sources. The SOD UoTs continue to contain a high volume of collections and disbursements which require manual research and resolution. That manual research and resolution supports the production of the final UoTs and materiality assessments but takes a significant amount of time making them unavailable for financial reporting. Additionally, at the time of UoT availability, there is a significant volume of transactions, for a significant dollar amount, making up the SOD balances that have not been identified to an entity and are listed in the UoTs as "TBD."

While DISA WCF'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: Without receiving the complete and final SOD UoTs from DISA WCF's service organization in a timely manner, DISA WCF is unable to identify its transactions that are included within SODs, if any, to recognize amounts within its accounting records in the period in which the transactions were processed. Further, without additional compensating controls and/or monitoring procedures, DISA WCF is unable to assert to the completeness and accuracy of reported FBWT on its Balance Sheet and other financial statement line items, as applicable.

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Coordinate with its service organization to continue to develop procedures to determine what portion of the SOD balances, if any, should be attributed to DISA WCF for financial reporting in a timely manner and made available for year-end financial reporting purposes.
2. Coordinate with its service organization to continue to monitor and track the resolution of SOD activity cleared to DISA WCF to enable the entity to perform root cause analysis. This includes further research and resolution over the transactions not resolved in the UoTs and listed as "TBD."
3. Coordinate with its service organization to continue to develop effective system and process controls to ensure that disbursements and collections are processed with valid TI, TAS, and FY inputs.
4. Coordinate with its service organization to assess and identify ALCs that primarily report collection and disbursement activity to Treasury on behalf of DISA WCF.
5. Coordinate with its service organization to monitor and track the resolution of SODs cleared to DISA WCF to enable the entity to perform root cause analysis and develop compensating controls for financial reporting purposes.
6. Coordinate with its service organization to continue coordinating recurring meetings with DISA WCF to help resolve outstanding differences.
7. Assist DISA WCF's service organization by providing supporting information to clear transactions reported in SODs timely.
8. Work with Treasury, the Office of the Secretary of Defense, DISA WCF's service organization, and other parties to transition away from using monthly NTDO reporting ALCs to daily TDO reporting ALCs.

9. Consider any limitations to DISA WCF's service organization's SOD process and develop compensating controls to reconcile SOD balances to minimize the risk of a potential material misstatement.
10. Pursuant to receiving the necessary information and documentation from DISA WCF's service organization, develop and implement procedures to identify DISA WCF's actual or estimated SOD balances for recording and reporting adjustments within the financial statements.

II. Property, Plant, and Equipment (*Repeat Condition*)

A. Untimely Asset Activation

Background: The June 30, 2024 DISA WCF General Property, Plant, and Equipment (PP&E) was composed of equipment, software, right-to-use lease assets, and Construction in Progress (CIP) with a net book value (NBV) of \$1.5 billion. DISA WCF utilizes the Defense Property Accountability System (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 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 WCF 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 journal voucher (JV) to account for the costs. DISA WCF is responsible for establishing controls to record assets timely and accurately in DPAS.

DISA WCF must record capital assets accurately in the correct accounting period. PP&E shall be recognized when the title passes to the acquiring entity or when PP&E is delivered to the entity or to an agent of the entity per SFFAS No. 6, *Accounting for Property, Plant, and Equipment*.

Condition: DISA WCF 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 WCF's PP&E account:

- DISA WCF did not record software with an NBV of \$573 thousand with a recorded activation date from FY 2023 in the correct FY

- DISA WCF did not transfer equipment with an NBV of \$1.8 million in transfers from GF to the WCF in the correct FY
- DISA WCF did not record \$151 thousand NBV of ancillary costs in the correct FY.

Cause: The untimely asset activation and transfers generally resulted from inconsistent or ineffective communications between program officials responsible for the assets and the DISA WCF officials who are responsible for property accounting. Additionally, due to DISA 's decentralized environment with equipment in locations worldwide, DISA personnel do not always provide documentation to the DISA CAM Team timely or have a consistent understanding of property accounting requirements.

Effect: The untimely asset activation and transfers resulted in an understatement of approximately \$2.5 million NBV on the PP&E line of the Balance Sheet and the General Equipment cost on Footnote 9 of the September 30, 2023 WCF financial statements. The untimely asset activation also resulted in an understatement of approximately \$155 thousand of depreciation on the Gross Costs line of the Statement of Net Cost. 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.

Recommendation: Kearney recommends that DISA WCF 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 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. 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.
5. Develop and implement a process to ensure and document that software is activated and recorded in the correct FY.

III. Information Technology (*Modified Repeat Condition*)

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

- A. Defense Information Systems Agency Risk Management Framework
- B. Financial Accounting Management Information System – Working Capital Fund Database Audit Logging and Monitoring
- C. Incomplete Financial Accounting and Budget System Application Access Request Documentation



D. Incomplete Complementary User Entity Controls Implementation

A. 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 WCF meets the DoD's information technology (IT) needs through enterprise security architectures, smart computing options, and other leading-edge IT opportunities. Specifically, DISA WCF delivers hundreds of IT support services capabilities and has the capacity to host, support, engineer, test, 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 (IS) 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 ISs and inherited by those systems.

DISA WCF utilizes Enterprise Mission Assurance Support (eMASS) to implement the RMF to its respective systems. eMASS is a web-based Government Off-the-Shelf 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 Instruction (CNSSI) No. 1253, *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 controls that are applicable to all NSSs.

The CNSS collaborates with NIST to ensure NIST SP 800-37 (as amended); NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*; 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.

NIST published SP 800-53, Rev. 5 on September 23, 2020 and SP 800-53A, Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, in January 2022. Per Office of Management and Budget (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.

On October 16, 2023, the DoD Chief Information Security Officer issued a memorandum announcing the DoD's adoption and transition timeline for Rev. 5 of the NIST SP 800-53 security controls and the corresponding control baselines in Rev. 5 of the CNSSI No. 1253. The memorandum states:

“As part of the adoption of Rev. 5, new systems, systems that have initiated RMF (but have not yet begun executing a security plan), and systems with an RMF authorization decision more than 3 years old should begin transition to Rev. 5 with[in] 6 months of the issuance of this memo [16 April 2024]. Systems that are currently executing the RMF security plan should either continue under Rev. 4 and develop a strategy and schedule for transition to Rev. 5 with the Authorizing Official's (AO) approval or begin transition to Rev. 5. Systems that have a current (within 3 years) RMF system authorization decision should develop a strategy and schedule for transition with the AO's approval. This schedule must not exceed the system re-authorization timeline.”

The memo also notes that the DoD transition timeline will be published on the RMF Knowledge Service (KS) at <https://rmfks.osd.mil>. The DoD transition timeline on the RMF KS states that eMASS updates were completed in January 2024.

Condition: DISA WCF did not update its RMF documentation, processes, procedures, or System Security Plans to reflect updated requirements presented within NIST SP 800-53, Rev. 5 in the prescribed timeline set forth by OMB Circular A-130, Appendix I. Furthermore, DISA WCF did not adhere to the guidance dictated in the DoD adoption memorandum. Specifically, the entity did not develop an official strategy and schedule for transition to NIST SP 800-53, Rev. 5 with AO approval.

Cause: As of July 2024, DISA WCF personnel began developing a plan detailing a phased approach to transition the Budget and Execution Reporting Tool (BERT), Financial Accounting Management Information System – Working Capital Fund (FAMIS-WCF), and Financial Accounting and Budget System (FABS) applications to NIST SP 800-53, Rev. 5. However, DISA WCF personnel stated that DISA WCF's ability to transition to NIST SP 800-53, Rev. 5 within eMASS is determined by the AO, who had not made the control set and functionality available to DISA WCF. Furthermore, DISA WCF personnel had not obtained a signed and approved strategy and schedule from the AO for transitioning to NIST SP 800-53, Rev. 5 control sets for BERT, FAMIS-WCF, and FABS.

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.

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Finalize an official strategy and schedule for transition to NIST SP 800-53, Rev. 5 with the AO's approval and within system re-authorization timelines or begin transition to Rev. 5, as required per the DoD Rev. 5 adoption memorandum.

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

Background: The DISA WCF Accounting Integration Branch is responsible for IS security management and audit logging and monitoring for FAMIS-WCF.

As a turn-key Financial Management System Software solution, FAMIS-WCF, based on Oracle eBusiness Suite (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 Procurement. The resulting system implements Oracle Identity and Access Management to interface with EBS to provide Common Access Card authentication to EBS.

According to NIST SP 800-92, *Guide to Computer Security Log Management*, 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 WCF utilizes Oracle to log configuration changes made to the FAMIS-WCF database. The FAMIS-WCF database administrators (DBA) have configured the database to automatically initiate daily e-mail-generated reports based on pre-defined criteria for analysis and review. Subsequently, the DBAs route the e-mail-generated reports to the appropriate personnel (i.e., Information System Security Manager) for analysis and review.

Condition: While DISA WCF implemented a process to log and review configuration changes to the FAMIS-WCF database daily, DISA WCF personnel did not adhere to the required review timeframe of seven days following the daily e-mail-generated audit log reports. Specifically, DISA WCF personnel did not perform timely reviews for 17 of the 37 (~46%) FAMIS-WCF database audit logs sampled for testing.

Cause: DISA WCF personnel implemented a process to log all configuration changes to the FAMIS-WCF database; however, DISA WCF failed to consistently perform timely reviews over the database audit logs, as 17 of the 37 sampled reviews (~46%) were not reviewed within the seven-day timeframe due to sudden and unexpected change in personnel. Additionally, DISA WCF had not defined back-up personnel to ensure reviews were completed in a timely manner.

Effect: By not reviewing FAMIS-WCF database audit logs in a timely manner, DISA WCF 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 WCF's ability to initiate prompt corrective action.

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Update the review process within the appropriate procedural and security documentation to include primary and back-up reviewers, as well as all personnel responsible for reconciliation.
2. Consistently perform reviews over the database audit logs in a timely manner as defined within FAMIS-WCF policies, as well as other Federal and/or DoD criteria (i.e., seven days).
3. Develop and implement a quality control (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.
4. Continue to retain evidence of the review of FAMIS-WCF database logs for third-party review.

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

Background: DISA WCF personnel located at Fort George G. Meade are responsible for information system security and account management for FABS. FABS manages and tracks the financial transactions associated with telecommunication circuits, equipment, and services leased from various vendors on behalf of the Government through the Telecommunications Services Enterprise Acquisition Services Defense Working Capital Fund. Financial transactions are sent from the Contracting Online Procurement System to FABS, which generate AP for vendor payment. FABS also supports customer billing, indicating monthly recurring charges, non-recurring charges, subscriber rate charges, usage charges, overhead charges, taxes, surcharges, and universal service fee.

DISA WCF controls initial account access to the FABS application through completion of a user access request form via Enterprise Security Posture System (ESPS)/System Access Management (SAM). To gain access to the FABS application, users will navigate to the ESPS/SAM to submit access request. This request requires the prospective user to have completed security awareness

training, provide required personal information, and include the approval signatures of the user's supervisor and the user's local Security Manager. The user's supervisor then routes the completed and auto-generated System Authorization Access Request (SAAR) forms to the System Administrator (SA) group to gather final approval from the FABS Data Owner (DO) for processing. The SA group identifies the applicable DO residing in DISA WCF's Office of Accounting Operations and Compliance or Defense Information Technology Contracting Organization – Scott Procurement Services Directorate (PL13). The DO then conducts the final review of the SAAR and signs the form, indicating approval.

NIST SP 800-53, Rev. 5 informs individuals responsible for ISs that approving and enforcing authorized access at the application provides increased information security. Unapproved and inappropriate user access and privileges increase the risk to the confidentiality, integrity, and availability of the system and its data.

Condition: DISA WCF was unable to provide sufficient documentation to support that management reviewed and approved access permissions for one of nine sampled FABS application accounts. Specifically, DISA WCF granted a new user access to an existing System Administrator account prior to obtaining the appropriate approvals.

Cause: Due to a prior FABS System Administrator leaving their position, DISA WCF personnel reused and renamed the privileged user account to grant access to the new System Administrator user access.

Effect: By failing to create new user accounts and utilizing existing accounts for new users, there is increased risk that users may receive inappropriate or unauthorized access to privileges and roles within the FABS application.

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Update and enforce a policy that restricts the renaming or modification of an existing user account for a different role. Each role should be a unique account to maintain proper accountability and traceability.
2. Develop and implement a QC review over the user authorization process. The QC process should include procedures to ensure completion of access request forms in ESPS/SAM for all FABS users and validation of requested roles. To gain efficiencies, DISA WCF should consider incorporating this QC process as it conducts its audit log reviews of account creations and modifications.

D. Incomplete Complementary User Entity Controls Implementation

Background: DISA WCF utilizes several service organizations to support its operations and mission. As such, DISA WCF 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 IS(s). These assertions are communicated via a System and Organization

Controls (SOC) report. In FY 2024, 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, the Statement on Standards for Attestation Engagements 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 WCF 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 WCF 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; the Defense Finance and Accounting Service's (DFAS) Defense Cash Accountability System (DCAS) for transaction distribution services; DFAS's Defense Civilian Pay System (DCPS) for Federal civilian payroll services; DFAS's Defense Departmental Reporting System (DDRS) for financial reporting services; DFAS's Automated Disbursing System (ADS) for standard disbursing services; Defense Manpower Data Center's Defense Civilian Personnel Data System (DCPDS) for processing payroll affecting civilian human resource transactions; Chief Digital and Artificial Intelligence Office Directorate for Business Analytics' Advancing Analytics (Advana) to support budgetary processes; and DFAS's Mechanization of Contract Administration Services (MOCAS) for managing procurement payment and entitlement determinations of contract data for delivery and other reporting.

DISA WCF should implement all CUECs required by its service organizations, as documented in the service organizations' SOC reports, per NIST SP 800-53, Rev. 5, Control SA-9, "External System Services," and GAO's *Standards for Internal Control in the Federal Government* (Green Book, 2014), Section 4.

Condition: DISA WCF has not implemented all CUECs required by its service organizations. Based on a subset of high-risk CUECs (e.g., cross-system segregation of duties [SD] and removals) required by DISA WCF's service organizations. Examples of control deficiencies indicating CUECs that DISA WCF has not fully implemented or are not operating effectively include the following:

- DISA WCF did not develop cross-system SD documentation to detail conflicts that may occur when personnel obtain access to multiple systems utilized by DISA WCF, to

include, but not be limited to, ADS, Advana, DAI, DCAS, DCPS, DCPDS, DDRS, DPAS, MOCAS, and WAWF

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

Cause: Although DISA WCF 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 2024 financial statement audit. DISA WCF has continued to refine its existing process, as documented within the CUEC Review Process narrative. Specifically, DISA WCF continues to identify and implement compensating controls to remediate control gaps identified during the reviews performed over the CUECs identified within each service organization’s SOC 1®, Type 2 report. Additionally, DISA WCF maps the relevant CUECs to the corresponding DISA WCF-performed control. Further, due to the large number of CUECs, DISA WCF established a phased approach and executed it to test CUECs based on level of risk and document results of implementation.

Effect: DISA WCF’s failure to implement internal controls to address all required CUECs may result in ineffective controls/control objectives. 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.

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Implement all CUECs identified within each service organization’s SOC 1®, Type 2 report.
2. Identify gaps for CUECs not designed and/or not operating effectively, as well as design and implement controls to remediate those gaps.

* * * * *



APPENDIX A: STATUS OF PRIOR-YEAR DEFICIENCIES

In the *Independent Auditor's Report on Internal Control over Financial Reporting* included in the Defense Information Systems Agency Working Capital Fund's fiscal year (FY) 2023 Agency Financial Report (AFR), we noted several issues that were related to internal control over financial reporting. The statuses of the FY 2023 internal control findings are summarized in *Exhibit 2*.

Exhibit 2: Status of Prior-Year Findings

Control Deficiency	FY 2023 Status	FY 2024 Status
Fund Balance with Treasury	Material Weakness	Significant Deficiency
Property, Plant, and Equipment	Significant Deficiency	Significant Deficiency
Budgetary Resources	Significant Deficiency	Not Applicable (N/A)
Financial Reporting	Significant Deficiency	N/A
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. 24-02, *Audit Requirements for Federal Financial Statements*, the financial statements and the related notes to the financial statements of the Defense Information Systems Agency (DISA) Working Capital Fund (WCF) as of and for the year ended September 30, 2024, which collectively comprise DISA WCF's financial statements, and we have issued our report thereon dated November 8, 2024.

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 DISA WCF's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of the financial statement amounts and disclosures, including the provisions referred to in Section 803(a) of the Federal Financial Management Improvement Act of 1996 (FFMIA). 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, exclusive of those referred to in FFMIA, disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 24-02.

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 Section 803(a) requirements related to Federal financial management system requirements, applicable Federal accounting standards, or application of the United States Standard General Ledger at the transaction level.



Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements and the results of that testing, and not to provide an opinion on the effectiveness of DISA WCF's compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 24-02 in considering DISA WCF's compliance. Accordingly, this report 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
November 8, 2024

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 final audit report for DISA's FY 2024 Working Capital Fund (WCF) financial statements.

We acknowledge the auditor-identified findings in the following key areas: 1) Fund Balance with Treasury, 2) Property, Plant and Equipment, and 3) Information Technology each of which, in the aggregate are considered significant deficiencies.

DISA made tremendous progress in FY 2024 ending the year with no material weaknesses and is focused on successful resolution of the remaining issues identified above during the upcoming audit cycle.

SPONSELLER.JU Digitally signed by
SPONSELLER.JUSTIN.C.125
STIN.C.1258339 8339246
246 Date: 2024.11.08 16:14:06
-05'00'

JUSTIN SPONSELLER
Director, Accounting and
Audit Operations

Appendix A- DISA Organizational Chart

Joint Service Provider

Joint Force Headquarter-DoDIN

DISA Director JFHQ-DoDIN Commander

Deputy Director

Procurement Services Directorate
Chief Financial Officer and Comptroller

Assistant to the Director

Chief of Staff

Workforce Services and Development Directorate

Digital Capabilities and Security Center

Cyber Security and Analytics
Joint Enterprise Services
Defense Spectrum Organization
Joint Interoperability Test Command

Hosting and Compute Center

Compute Operations
Operations Support
Product Management

Enterprise Operations and Infrastructure Center

Endpoint Services and Customer Support
Transport Services
Cyberspace Operations

Enterprise Integration and Innovation Center

Emerging Technology and Enterprise Architecture
Enterprise Engineering and Governance
Risk Management Executive
Chief Data Officer

Special Staff

Chaplain Program Office
Congressional Affairs Coordinator
Office of Strategic Communication and Public Affairs
General Counsel
Inspector General
Component Acquisition Executive
Small Business Programs
Protocol
Pentagon Liaison Officer
Office of Equality, Diversity and Inclusion

ADCON Organizations

Joint Artificial Intelligence Center
Secretary of Defense Communications
White House Communications Agency
White House Situation Support Staff