

**Defense Information Systems Agency  
Working Capital Fund  
Agency Financial Report  
Fiscal Year 2023**



## 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, 2023. 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, Financial Reporting Requirements, to incorporate necessary operational and financial reporting process changes that validate our financial statements are complete, accurate and reliable.

Among DISA's FY 2023 highlights, we continued to lead the Department's transition to a cloud environment and enhanced cybersecurity architecture, including deployment of a classified DoD365 tenant for consistent communication, collaboration, and productivity capabilities across networks; investing in enhanced MS365 licensing for improved zero trust; and implementation of the Joint Warfighting Cloud Capability. DISA plays a role in nearly every combat engagement and aids humanitarian assistance, disaster relief, and intelligence and special operations activities, including support in Ukraine's conflict.

DISA's actions in support of our Strategic Plan FY 2024-2026 will continue to implement, sustain, and evolve the global network infrastructure and unified capabilities to provide information superiority to the President; the Secretary of Defense; combatant commanders; senior leadership; Military Services; Defense Agencies; and the warfighter. Key focus areas throughout these LOEs include delivering the right capability at the right time, improving efficiency and effectiveness; reducing time to deliver solutions; standardizing services; and delivering best value capabilities both internally and for our mission partners. Sound financial processes and practices and reliable data are foundational to meeting our strategic objectives.

This year, we have continued to make improvements in our financial processes based on feedback by our independent public accounting firm Kearney & Company. DISA can provide reasonable assurance that internal controls over financial reporting, operations, and compliance are operating effectively as of Sept. 30, 2023. We continued progress addressing significant deficiencies and material weaknesses on DISA's WCF financial statements. Information obtained through this year's report and continued improvements leverage our ongoing efforts to improve all aspects of DISA's WCF. DISA continues to evolve our financial processes, improving accuracy and efficiency for better decision making. DISA will continue to gain efficiencies by expanding our usage of robotic process 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 that reads "Robert J. Skinner".

ROBERT J. SKINNER  
Lieutenant General, USAF  
Director

## Table of Contents

<b>Management’s Discussion and Analysis.....</b>	<b>1</b>
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
<b>Principal Statements.....</b>	<b>34</b>
<b>Notes to the Principal Statements.....</b>	<b>39</b>
<b>Required Supplementary Information.....</b>	<b>56</b>
Deferred Maintenance and Repairs Disclosures.....	57
<b>Other Information.....</b>	<b>59</b>
Management Challenges.....	62
Payment Integrity.....	72
<b>DOD Office of Inspector General (OIG) Audit Report Transmittal Letter.....</b>	<b>73</b>
<b>Independent Auditor’s Report.....</b>	<b>76</b>
<b>DISA Management Comments to Auditors Report.....</b>	<b>112</b>
<b>Appendix A.....</b>	<b>114</b>

# **DISA Working Capital Fund Fiscal Year 2023**

## **Management's Discussion and Analysis**

The Defense Information Systems Agency (DISA) is pleased to present a Management Discussion and Analysis (MD&A) to accompany its fiscal year (FY) 2023 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 to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations. DISA implements the Secretary of Defense's Defense Strategic Guidance 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."

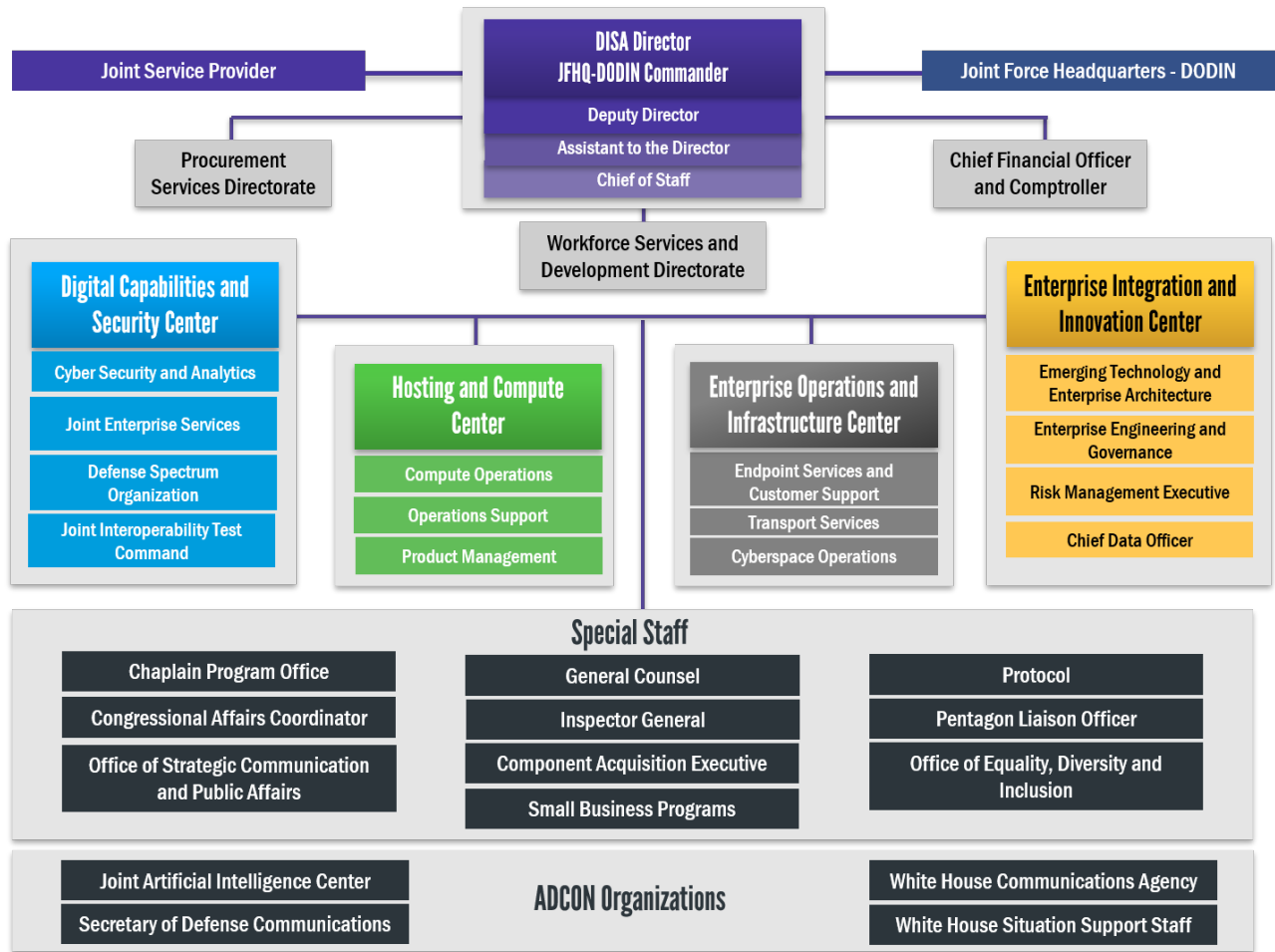
DISA serves the needs of the president, vice president, secretary of defense, Joint Chiefs of Staff (JCS), combatant commands, and other DOD components during peace and war. In short, DISA provides global net-centric solutions in the form of networks, computing infrastructure, and enterprise services 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 July 2023 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 Working Capital Fund (WCF) relies on revenue earned from

providing IT and telecommunications services and capabilities to finance specific operations. Mission partners order capabilities or services from DISA and make payment to the WCF when the capabilities or services are received.

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

DISA operates the information services activity within the DWCF. This activity consists of two main components. The first component includes two lines of service: Telecommunications Services and Enterprise Acquisition Services (TSEAS) (PE55/56). The second component includes Computing Services (CS) (PE54).

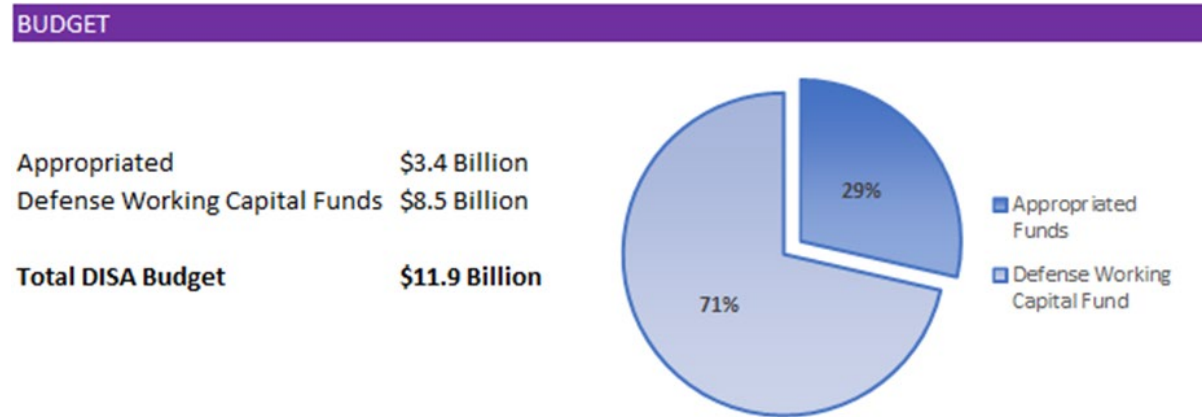
The major element of the Telecommunication Services (TS) component is the Defense Information Systems Network (DISN), which provides interoperable telecommunications connectivity and accompanying services that allow the department to plan and operate both day-to-day business and operational missions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

The line of service for Enterprise Acquisition Services (EAS) (PE56) enables the department to procure best value, commercially competitive IT services and capabilities through DISA's Defense IT Contracting Organization (DITCO). DITCO provides complete contracting support and services.

The major programs in FY 2023 for DISA WCF are Enterprise Acquisition Services IT Contracts, Joint Enterprise Level Agreements (JELA), Computing Services and Commercial Satellite. Due to normal business operations, major programs may change from year to year.

The Computing Services component of DISA's DWCF activities operates DISA data centers, which provide mainframe and server-processing operations, data storage, production support, technical services, and end-user assistance for command and control, combat support, and enterprise applications across DOD. These facilities and functions provide a robust enterprise computing environment to more than 4 million users through 17 mainframes; more than 13,000 servers; 110,000 terabytes of data; and approximately 219,000 square feet of raised floor.

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





## **Global Presence**

DISA is a global organization of approximately 7,500 civilian employees; 1,700 active-duty military personnel from the Army, Air Force, Navy, and Marine Corps; and over 11,000 defense contractors. This data is as of Sept. 2023. 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 charged with the responsibility for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the president, the vice president, the secretary of defense, and the DOD components under all conditions of peace and war.

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

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

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



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

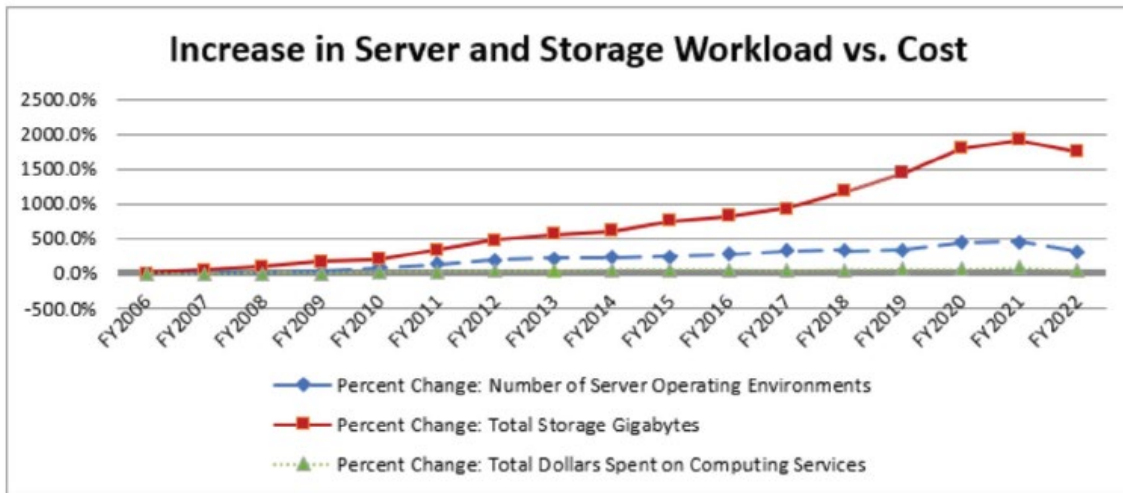
***Program Performance***

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

**DISA Working Capital Fund (WCF) Performance Measures**

The table below represents the increased demand for DISA’s server and storage computing services, which has grown significantly since FY 2006. Since that year, the number of customer-driven server operating environments has increased by 327 percent, and total storage gigabytes have increased by 1,789 percent. Over the same timeframe, the cost to deliver all computing services has increased by only 36

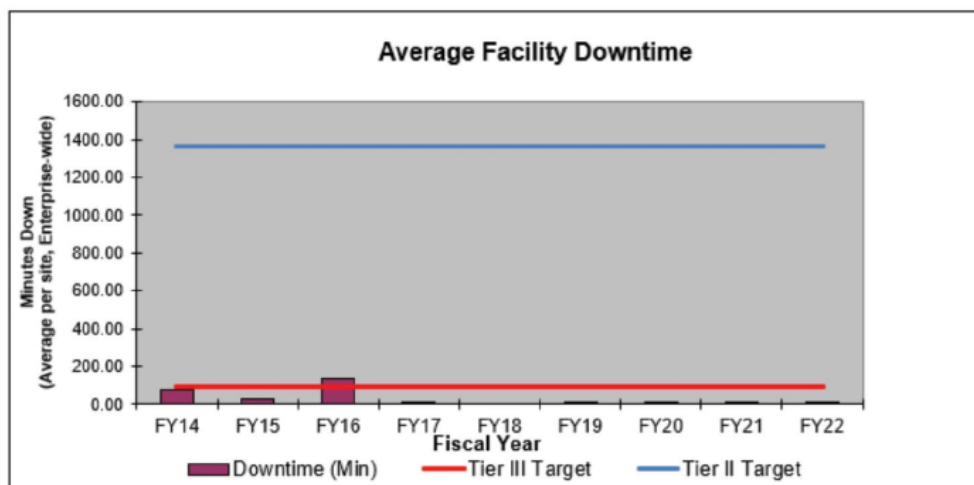
percent. In short, customers are demanding considerably more services and are at the same time benefiting from DISA’s unique ability to leverage robust computing capacity at DISA data centers.



The Computing Services business area tracks its performance and results through the agency director’s Quarterly Performance Reviews. There are two key operational metrics that are presented to DISA director in conjunction with regular, recurring Quarterly Program Reviews. These two metrics depicted in the following tables reflect the availability of critical applications in the Core Data Centers.

The first metric, “Core Data Center Availability,” expressed in minutes per year, represents application availability from the end user’s perspective and includes all outages or downtime regardless of root cause or problem ownership. Tier II requires achieving 99.75 percent availability, which limits downtime to approximately 1,361 minutes per year. Tier III, the standard for all DOD-designated Core Data Centers, requires achieving 99.98 percent availability, which limits downtime to approximately 95 minutes per year.

**Core Data Center Availability**



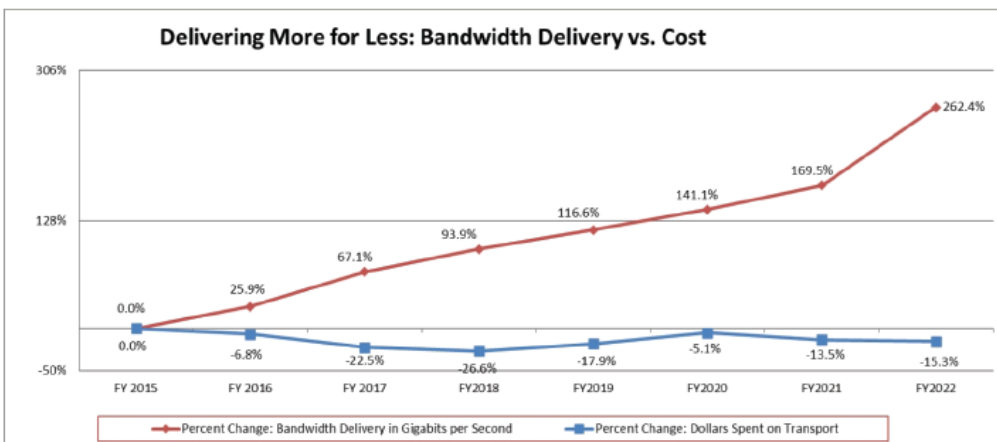
The second metric, “Capacity Service Contract Equipment Availability,” represents DISA’s equipment availability by technology, i.e., how well DISA is executing its responsibilities exclusive of factors

outside the agency's control such as last-mile communications issues, base power outages, or the like. The “threshold” refers to system uptime and capacity availability for intended use; this is the level required by contract. The “objective” is the value agreed on by the vendor and the government to be an ideal target, and the vendor reports the actual value on a monthly basis.

**Figure 1-Capacity Services Contract Equipment Availability**

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

The Telecommunications Services business area provides a set of high quality, reliable, survivable, and secure telecommunications services to meet the department’s command and control requirements. The major component of Telecommunications Services is the DISN, a critical element of the DODIN that provides the warfighter with essential access to timely, secure, and operationally relevant information to ensure the success of military operations. The DISN is a collection of robust, interrelated telecommunications networks that provide assured, secure, and interoperable connectivity for the DOD, coalition partners, national senior leaders, combatant commands, and other federal agencies. Specifically, the DISN provides dynamic routing of voice, data, text, imagery (both still and full motion), and bandwidth services. The robustness of this telecommunications infrastructure has been demonstrated by DISA’s repeated ability to meet terrestrial and satellite surge requirements in southwest Asia while supporting disaster relief and recovery efforts throughout the world. Overall, the DISN provides a lower customer price through bulk quantity purchases, economies of scale, and reengineering of current communication services. In spite of this continuing upward trend in demand, DISA has delivered transport services at an overall cost decrease to mission partners, as shown in the subsequent chart:



The previous chart compares the bandwidth delivery, including multiprotocol label switching connections, with transport costs. Since FY 2015, DISA has increased transport bandwidth delivery capacity 262.4 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 15.3 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**

<b>SERVICE OBJECTIVE</b>	<b>FY 2022 ACTUAL</b>	<b>FY 2023 Operational Goal</b>	<b>FY 2024 Operational Goal</b>
Non-Secure Internet Protocol Router Network access circuit availability	99.78%	98.50%	98.50%
Secure Internet Protocol Router Network latency (measurement of network delay) in the continental United States	40.31 Milliseconds	<= 100 milliseconds	<= 100 milliseconds
Optical Transport network availability	99.66%	99.50%	99.50%

The EAS business area is the department’s ideal source for procurement of best-value and commercially competitive IT. EAS provides contracting services for IT and telecommunications acquisitions from the commercial sector and contracting support to the DISN programs, as well as to other DISA, DOD, and authorized non-defense customers. These contracting services are provided through DISA’s 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**

<b>SERVICE OBJECTIVE</b>	<b>FY 2022 ACTUAL</b>	<b>FY 2023 Operational Goal</b>	<b>FY 2024 Operational Goal</b>
Percent of total eligible contract dollars completed	85.60%	73.00%	73.00%
Percent of total eligible contract dollars awarded to small businesses	25.29%	25.00%	25.00%

\*FY 2023 and FY 2024 goals for percent of total eligible contract dollars completed are estimates based on the released FY 2022 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 Dec. 21, 2023.

## **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.

DISA Working Capital Fund (WCF) did not receive a significant amount of COVID related budgetary resources in fiscal year (FY) 2023. DISA WCF does not have any existing indefinite resources associated with COVID requirements. In FY 2023, there was no additional impact to financial reporting for DISA WCF assets, liabilities, cost, revenue, or net position.

### ***Defense Working Capital Fund Financial Highlights***

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

### **Executive Summary**

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 decrease \$33.1 million for a total of \$370.6 million on its unobligated balance available, as compared with the fourth quarter of FY 2022.

- The Statement of Net Cost reflects a loss through the fourth quarter of FY 2023 of \$67.8 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 \$504.3 million, in comparison with the fourth quarter of last year.
- Cash levels remained positive through the fourth quarter of FY 2023 at 11.9 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 2023 reported balances and the fourth quarter of FY 2022. Balances that have the same underlying explanation between budgetary and proprietary accounts are explained from the proprietary perspective and referenced from the budgetary perspective. Due to rounding, tables in this document may not add to overall totals.

**STATEMENT OF NET COST**

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

*Gross Cost* - Gross Cost totaling \$8.1 billion increased \$164.5 million (2 percent) between the fourth quarter of FY 2022 and the fourth quarter of FY 2023. 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 for FY 2023 and presented as one consolidated program for the purpose of financial reporting.

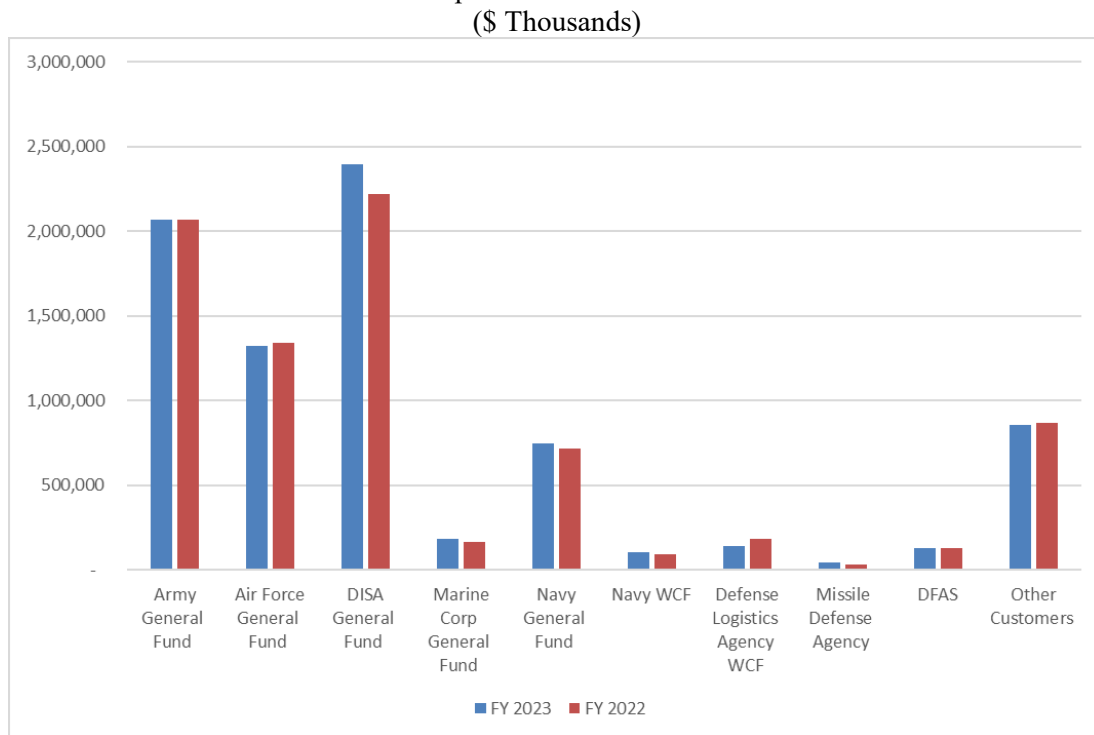
**Figure 4- Gross Cost**

	(thousands)			
DISA WCF (thousands)	9/30/2023	9/30/2022	Inc/Dec	% Chg.
<b>Total Gross Cost</b>	\$ 8,063,925	\$7,899,437	\$ 164,489	2%
Less: Earned Revenue	(7,996,143)	(7,808,452)	(187,692)	2%
<b>Total DISA WCF Operating Cost</b>	\$ 67,782	\$ 90,985	\$ 23,203	-26%

*Earned Revenue* - Earned Revenue totaling \$8.0 billion increased \$187.7 million (2 percent) between the fourth quarter of FY 2022 and the fourth quarter of FY 2023.

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

The bar chart below reflects earned revenue per customer for FY 2023 and FY 2022.



*Net Cost of Operations* – Net Cost of Operations decreased \$23.2 million (26 percent) between the fourth quarter of FY 2022 and the fourth quarter of FY 2023 due to the increase in earned revenue of

\$187.7 million as well the increase in gross cost of \$164.5 million between fiscal years.

**Figure 5-Net Cost of Operations**

(thousands)				
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
CS	\$ (8,079)	\$ (62,991)	\$ 54,912	-87%
TSEAS	110,015	186,845	(76,830)	-41%
Component	( 34,154)	(32,869)	(1,285)	4%
<b>Total</b>	<b>\$ 67,782</b>	<b>\$ 90,985</b>	<b>\$ (23,203)</b>	<b>-26%</b>

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

- Telecommunication Services (TS) Transport Capital net cost increased \$25.8 million as a result of changes in depreciation due to the timing of capital projects.
- TS Commercial Satellite net cost increased \$19.4 million because of an increase in customer demand.
- CS Server/Storage Infrastructure net cost decreased \$26.3 million because of a delay in facilities projects as well as under execution of contract labor and server hardware capacity services.
- Enterprise Acquisition Services (EAS) Telecommunications Contracts net cost decreased \$21.0 million. These are pass-through contracts which are driven entirely by customer demand and will fluctuate from year-to-year based on who the customer chooses to use for their contracting needs.
- EAS Information Technology Contracts net cost decreased \$17.3 million. These are pass-through contracts which are driven entirely by customer demand and will fluctuate from year-to-year based on who the customer chooses to use for their contracting needs.
- TS 4ENO Dedicated Services net cost decreased \$15.1 million due to timing of billing for 4ENO direct reimbursable services, such as one-time migration costs.

**BALANCE SHEET**

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

**Assets**

Total assets of \$2.2 billion comprise primarily Fund Balance with Treasury (\$305.1 million); Intragovernmental Accounts Receivable (\$873 million); and General Property, Plant, and Equipment (PP&E) (\$1 billion).

*Fund Balance with Treasury* - Fund Balance with Treasury Inception to Date (ITD) Balance decreased \$33.1 million (10 percent) over last year. The following chart displays fiscal year to date (FYTD) net cash flow from current year operations (collections less disbursements) reported to Treasury for FY 2023 and FY 2022, as reflected in the monthly AR(M) 1307 Cash Flow report, presented in a comparative manner:



**Figure 6-Fund Balance with Treasury**

	(thousands)			
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
CS Beginning Balance	\$ 49,946	\$ 31,709	\$ 18,237	58%
CS YTD	745,193	770,038	(24,845)	-3%
<b>CS Total</b>	<b>795,139</b>	<b>801,747</b>	<b>(6,608)</b>	<b>-1%</b>
TS Beginning Balance	288,272	181,944	106,328	58%
TS YTD	(778,269)	(645,473)	(132,796)	21%
<b>TS Total</b>	<b>(489,997)</b>	<b>(463,529)</b>	<b>(26,468)</b>	<b>6%</b>
Total Beginning Balance	338,218	213,653	124,565	58%
YTD	(33,075)	124,565	(157,640)	-127%
<b>Total ITD Balance</b>	<b>\$ 305,143</b>	<b>\$ 338,218</b>	<b>\$ (33,075)</b>	<b>-10%</b>

- The \$305.1 million cash balance on Sept. 30, 2023, is composed of a \$338.2 million current year beginning balance and a FYTD \$33.1 million decrease from current year operations (includes capital outlays).
- The current year \$33.1 million decrease in fund balance results in a \$13.4 million positive variance when compared with the \$46.5 million forecasted decrease, as reflected in the Budget Executive Summary Cash Plan. Actual disbursements were \$326.8 million under plan, and actual collections were \$313.4 million under plan.
- The WCF decrease in cash from operations of \$33.1 million (10 percent) from Sept. 30, 2022, to Sept. 30, 2023, is consistent with normal business trends for accounts receivable and accounts payable fluctuations.
- The \$305.1 million WCF ITD cash balance represents approximately 11.9 days of cash on hand on Sept. 30, 2023, which was formulated by dividing \$305.1 million by the daily cash calculation amount of \$25.7 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 increased \$137 million (19 percent). The largest increase was within the TSEAS intragovernmental receivables. This amount included decreases due to the transfer of CS receivables, and in EAS, Telecommunications Contracts, ELA, and Defense Business Systems. These decreases were offset by increases in EAS, Contracting and Acquisition Support, and in Telecommunication Services (TS), Reimbursable Telecommunications Services, Transport Services, Cybersecurity Services, and Defense Information Systems Network (DISN) Infrastructure Service Revenue.

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

**Figure 7-Accounts Receivable, Net**

		(thousands)			
DISA WCF		9/30/2023	9/30/2022	Inc/Dec	% Chg.
<b>CS</b>					
Intragovernmental	\$	0	\$ 176	\$ (176)	-100%
Public		0	5	(5)	-100%
<b>TS</b>					
Intragovernmental		872,973	735,726	137,248	19%
Public		875	942	(67)	-7%
<b>Total</b>					
Intragovernmental		872,973	735,902	137,072	19%
Public		875	947	(72)	-8%
<b>Total Accounts Receivable</b>	\$	<b>873,849</b>	<b>\$ 736,849</b>	<b>\$ 137,000</b>	<b>19%</b>

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

**Figure 8-General PP&E, Net**

		(thousands)			
DISA WCF		9/30/2023	9/30/2022	Inc/Dec	% Chg.
CS	\$	0	\$ 17,356	\$ (17,356)	-100%
TSEAS		1,011,565	998,216	13,349	1%
<b>Total</b>	\$	<b>1,011,565</b>	<b>\$ 1,015,572</b>	<b>\$ (4,007)</b>	<b>0%</b>

- PP&E decreased \$4 million and is mainly due to the decrease in General Equipment, Software and transfer out of leasehold improvements, offset by an increase in construction-in-progress (CIP). The change in CIP is due to an increase in receipts for capital purchases related to the DISN, which was previously funded under the GF.
- Non-recoverable depreciation expenses decreased \$1.6 million 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.

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

**Figure 9- PP&E-Net Book Value**

(thousands)				
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
<b>Net Book Value</b>	\$1,011,565	\$ 1,015,572	\$ (4,007)	
TSEAS DPAS Values	436,211	332,259	103,952	31%
Optical Transport Network	62,208	50,016	12,192	24%
Fiber IRUs	26,599	27,408	(809)	-3%
Joint Regional Security Stacks	156,419	198,102	(41,683)	-21%
TSEAS Assets Pending	126,250	145,324	(19,074)	-13%
CS PP&E	0	17,356	(17,356)	-100%
Multiprotocol Label Switching	11,957	31,256	(19,299)	-62%
<b>Subtotal</b>	<b>\$ 819,644</b>	<b>\$ 801,722</b>	<b>\$ 17,922</b>	<b>2%</b>
Non-Recoverable Depreciation	182,640	184,198	(1,558)	-1%
<b>NBV of Remaining Programs</b>	<b>\$ 9,281</b>	<b>\$ 29,651</b>	<b>\$ (20,370)</b>	<b>-69%</b>

*Other Assets* – Advances and prepayments decreased \$257.2 thousand (100 percent) within TSEAS due to a prior year adjustment made to reconcile trading partner data. A current fiscal year adjustment was not required due to trading partner reconciliations with DISA WCF.

**Figure 10-Other Assets**

(thousands)				
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
Public	0	257	(257)	-100%
<b>Total</b>	<b>\$ 0</b>	<b>\$ 257</b>	<b>\$ (257)</b>	<b>-100%</b>

### **Liabilities**

Total liabilities of \$1 billion is composed primarily of intragovernmental accounts payable (\$46.1 million), intragovernmental other liabilities (\$2.7 million), non-federal accounts payable (\$907.2 million), other federal employment benefits (\$5.3 million), and non-federal other liabilities (\$47.1 million).

*Total Liabilities Not Covered by Budgetary Resources* – Total liabilities not covered by budgetary resources decreased \$789 thousand (16 percent) and consisted of other liabilities and the military retirement benefits.

**Figure 11-Total Liabilities Not Covered by Budgetary Resources**

(thousands)				
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
TSEAS	5,794	5,005	789	16%
<b>Total</b>	<b>\$ 5,794</b>	<b>\$ 5,005</b>	<b>\$ 789</b>	<b>16%</b>

*Total Liabilities Covered by Budgetary Resources* – Total liabilities covered by budgetary resources increased \$21.7 million (2 percent). The largest portion of the balance is made up of EAS, IT contracts.

The table below compares current year with prior year liabilities covered by budgetary resources and includes the public accounts payable balances.

**Figure 12-Total Liabilities Covered by Budgetary Resources**

(thousands)				
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
CS	\$ 1,957	\$ 13,431	\$ (11,474)	-85%
TSEAS	1,000,735	967,519	33,216	3%
<b>Total</b>	<b>\$ 1,002,692</b>	<b>\$ 980,950</b>	<b>\$ 21,742</b>	<b>2%</b>

From a customer funding perspective, DISA GF and Army continue to provide the most customer-funded contract requirements associated with the public accounts payable balance. The change in the accounts payable balance is primarily attributed to increases in EAS, Enterprise License Agreements and Telecommunications Contracts, and CS, Capacity Services. These are offset by decreases in EAS, IT Contracts and TS, Delivery Services.

*Other Liabilities* - Other Liabilities increased \$1.3 million (3 percent), primarily driven by the increase of accrued funded payroll and leave in TSEAS.

**Figure 13-Other Liabilities**

(thousands)				
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
<b>CS</b>				
Public	3,663	3,706	(43)	-1%
<b>TS</b>				
Intragovernmental	2,738	2,746	(8)	0%
Public	43,426	42,060	1,366	3%
<b>Total</b>				
Intragovernmental	2,738	2,746	(8)	0%
Public	47,089	45,766	1,323	3%
<b>Total Other Liabilities</b>	<b>\$ 49,827</b>	<b>\$ 48,512</b>	<b>\$ 1,315</b>	<b>3%</b>

## **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 \$89.5 million (45 percent) primarily in TS, 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 2023. Additionally, there were current year reversals of prior year activity that also contributed to the change.
- Imputed financing costs absorbed by others increased \$12.4 million (54 percent) due to the current fiscal year increase in employee imputed cost for life, health, and retirement.
- Net Cost of Operations decreased \$23.2 million (26 percent) as discussed in the Statement of Net Cost section.

## STATEMENT OF BUDGETARY RESOURCES

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

**Figure 14-Statement of Budgetary Resources**

	(thousands)			
DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
<b>CS</b>				
Obligations Incurred	\$ (46,801)	\$ (164,459)	\$ 117,658	-72%
Unobligated Balances	779,774	786,711	(6,937)	-1%
Contract Authority	(39,576)	(300)	(39,276)	13092%
Unfilled Customer Orders	0	3,273	(3,273)	-100%
Net Outlays	6,607	(123,452)	130,059	-105%
<b>TS</b>				
Obligations Incurred	8,090,199	5,474,114	2,616,085	48%
Unobligated Balances	(409,209)	(678,903)	269,694	-40%
Contract Authority	152,616	188,381	(35,765)	-19%
Unfilled Customer Orders	873,053	520,617	352,436	68%
Net Outlays	26,468	(1,112)	27,580	-2480%
<b>Component</b>				
Obligations Incurred	0	2,229,415	(2,229,415)	-100%
<b>Total</b>				
Obligations Incurred	\$ 8,043,398	\$ 7,539,070	\$ 504,328	7%
Unobligated Balances	\$ 370,566	\$ 107,808	\$ 262,758	244%
Contract Authority	\$ 113,040	\$ 188,081	\$ (75,041)	-40%
Unfilled Customer Orders	\$ 873,053	\$ 523,890	\$ 349,163	67%
Net Outlays	\$ 33,075	\$ (124,564)	\$ 157,639	-127%

*New Obligations and Upward Adjustments (line 2190)* - Obligations incurred increased \$504.3 million (7 percent). The major drivers for obligations incurred for DISA WCF are as follows:

- The largest increases for TSEAS were in Microsoft Joint Enterprise License Agreement (JELA), Commercial Satellite Services, and IT Contracts.
- The largest increase for CS was in Global Service Desk, Special Services Dedicated Labor Support and Data Center POH.

*Unobligated Balance, End of Period (line 2490)* - The unobligated balance as of Sept. 30, 2023, increased \$262.8 million (244 percent) between fiscal years. This is due to more obligations incurred compared with orders received within TSEAS, specifically in IT Contracts. Unobligated Balance, End of Period reflects the remaining balance in the following accounts at the end of the period; Allotments – Realized (USSGL 4610), and Commitments – Subject to Apportionment (USSGL 4700).

*Contract Authority (line 1690)* - Contract authority decreased \$75 million (40 percent) between fiscal years due to DISA WCF receiving more indefinite contract authority, offset by current fiscal year obligations being less than the prior fiscal year. The unused portion of contract authority is expected to be requested as carryover for FY 2024.

*Unfilled Customer Orders (USSGL 4221)* - Unfilled customer orders increased \$349.2 million

(67 percent) between fiscal years primarily in EAS IT Contracts.

*Outlays, Net (Line 4190)* – Net Outlays increased \$157.7 million (127 percent) between fiscal years and is reported as positive in this fiscal year due to disbursements being higher than collections.

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

### **RECONCILIATION OF NET COST TO NET OUTLAYS**

The purpose of the reconciliation of Net Costs to Outlays is to explain how budgetary resources applied during the period relate to the net cost of operations for the reporting entity. This information is presented in a way that clarifies the relationship between the outlays reported through budgetary accounting and the accrual basis of financial (i.e., proprietary) accounting. By explaining this relationship, the reconciliation provides the information necessary to understand how the budgetary outlays finance the net cost of operations and affect the assets and liabilities of the reporting entity. Most variances on this note are addressed in other sections.

**Figure 15-Net Cost of Operations**

		(thousands)		
DISA WCF 2023		Intragovernmental	Public	Total
<b>Net Cost of Operations</b>				
<b>Components of Net Cost Not Part of Net Outlays:</b>				
	\$	(7,708,698)	\$ 7,776,480	\$ 67,782
Property, Plant, and Equipment, net changes		0	(4,007)	(4,007)
Increase/(Decrease) in Assets:				
Accounts and taxes receivable, net		137,071	(72)	136,999
Other Assets		0	(257)	(257)
Increase/(Decrease) in liabilities:				
Accounts Payable		(8,219)	(12,412)	(20,631)
Federal employee benefits payable		0	(900)	(900)
Other liabilities		265	(1,265)	(1,000)
Other Financing Sources:				
Imputed cost		(35,453)	0	(35,453)
<b>Total Components of Net Cost That Are Not Part of Net Outlays</b>	<b>\$</b>	<b>93,664</b>	<b>\$ (18,913)</b>	<b>\$ 74,751</b>
<b>Miscellaneous Reconciling Items</b>				
Transfers (in)/out without reimbursements		(109,458)	0	(109,458)
Total Other Reconciling items		(109,458)	0	(109,458)
<b>Total Net Outlays</b>	<b>\$</b>	<b>(7,724,492)</b>	<b>\$ 7,757,567</b>	<b>\$ 33,075</b>
<b>Agency Outlays, Net, Statement of Budgetary Resources</b>				<b>\$ 33,075</b>
<b>Unreconciled difference</b>				<b>\$ 0</b>

**Figure 16-Illustrative Table of Key Measures**

(thousands)

DISA WCF	9/30/2023	9/30/2022	Inc/Dec	% Chg.
<b>COSTS</b>				
Gross Program Costs	\$ 8,063,925	\$ 7,899,437	\$ 164,489	2%
Less: Earned Revenue	7,996,143	7,808,452	187,692	2%
<b>Net Cost of Operations</b>	<b>67,782</b>	<b>90,985</b>	<b>(23,203)</b>	<b>-26%</b>
<b>NET POSITION</b>				
Assets:				
Fund Balance with Treasury	305,143	338,218	(33,075)	-10%
Accounts Receivable, Net	873,848	736,849	136,999	19%
Property, Plant & Equipment, Net	1,011,565	1,015,572	(4,007)	0%
Other	0	257	(257)	-100%
<b>Total Assets</b>	<b>2,190,556</b>	<b>2,090,895</b>	<b>99,661</b>	<b>5%</b>
Liabilities:				
Accounts Payable	953,381	932,750	20,631	2%
Federal Employee Benefits Payable	5,276	4,376	900	21%
Other Liabilities	49,827	48,512	1,315	3%
Other	2	316	(314)	-99%
<b>Total Liabilities</b>	<b>1,008,486</b>	<b>985,954</b>	<b>22,532</b>	<b>2%</b>
<b>Net Position (Assets minus Liabilities)</b>	<b>\$ 1,182,070</b>	<b>\$ 1,104,941</b>	<b>\$ 77,129</b>	<b>7%</b>

## **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.

## **2. Analysis of Systems, Controls, and Legal Compliance**

### ***Management Assurances***

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

Reviews, testing, and evaluations are conducted to assess if the internal control structure is 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 is providing reasonable assurance that our internal controls over reporting, operations, and compliance are operating effectively. Reasonable assurance has been achieved. This position on reasonable assurance is within the limits described in the preceding paragraph.



NOV 06 2023

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

SUBJECT: Annual Statement of Assurance Required Under the Federal Managers' Financial Integrity Act (FMFIA) for Fiscal Year (FY) 2023

As Director of the Defense Information Systems Agency (DISA), I recognize the DISA is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act (FMFIA) of 1982. DISA conducted its assessment of risk and internal control in accordance with the Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control" and the Green Book, 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, 2023. In FY 2023, there were six categories of material weaknesses (MWs) and Significant Deficiencies (SDs) that are in process of correction or 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 the DISA conducted this assessment. 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, the DISA can provide reasonable assurance that internal controls over operations and compliance are operating effectively as of September 30, 2023.

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 the DISA conducted this assessment. This assessment also included an evaluation of the internal controls around our Security Assistance Accounts (SAA) activities. Based on the results of the assessment, the DISA can provide assurance that internal controls over reporting (including internal and external reporting) as of September 30, 2023, and compliance are operating effectively as of September 30, 2023.

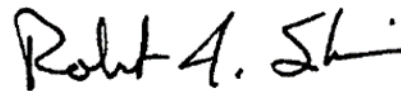
DISA Memo, *Annual Statement of Assurance Required Under the Federal Managers' Financial Integrity Act (FMFIA) for Fiscal Year (FY) 2023*,

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 the DISA conducted this assessment. This internal review also included an evaluation of the internal controls around our Security Assistance Accounts (SAA) activities. Based on the results of this assessment, the 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, 2023.

DISA has 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 Security Assistance Accounts (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, 2023.

DISA is hereby reporting that no Anti-Deficiency Act (ADA) violations have been discovered/identified during our assessments of the applicable processes OR Anti-Deficiency Act (ADA) violation(s) has (have) been discovered/identified during our assessments of the applicable processes.

If there are any questions regarding this Statement of Assurance for FY 2023, my point of contact is Mr. Alex Diaz, and he can be reached at alexis.diaz20.civ@mail.mil or (614) 692-9400.



ROBERT J. SKINNER  
Lieutenant General, USAF  
Director

Attachments:  
As stated

### ***FY 2023 Internal Control Program Initiatives and Execution***

In addition to the foundational sources of guidance such as OMB Circular A-123 and the GAO Green Book, DISA also receives direction from and coordinates with the Office of Under Secretary of Defense Comptroller (OUSD [C]) to execute its Risk Management Internal Control (RMIC) Program. The OUSD Comptroller RMIC Team issues the FY 2023 DOD Statement of Assurance Handbook that requires deliverables throughout the reporting cycle. The handbook provides practical guidance to carry out the program. In FY 2022, there was an emphasis on Entity Level Controls (ELCs), auditor Notice of Findings and Recommendations (NFR), Corrective Action Plan (CAP) implementation and resolution, and testing to pave the way in support of CAP resolution or mitigation. This remains in FY 2023; 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. In the course of the year, DISA will have submitted an End-to-End Process Control Narrative Key Controls Memo, Agency Risk Assessment, Material Weakness (MW) and Deficiencies Reporting and Removal Template, Entity Level Control Testing Validation, Fraud Controls Matrix, Complementary User Control CAPs, Summary of Management's Approach to Internal Control Evaluation Template, and a DATA Act Data Quality Controls Matrix in support of the program.

#### ***Correction of Prior Year Significant Deficiencies and Material Weaknesses:***

One of the department's focus areas is to make progress towards resolution of prior year MWs and conditions impeding audit progress. DISA has made concentrated efforts to resolve and clear prior year issues. In FY 2023, at the time of this memorandum, DISA has a potential to close 9 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 adheres to the NDBOP goal of "undergo an audit and improve the quality of budgetary and financial information that is most valuable in managing the DOD," through its audit and environment of continuous improvement and process refinement. The RMIC Program is managed through a three-tiered approach, which provides a structure to identify risk at an enterprise level, as well as at a more granular level. DISA director provides a "tone-at-the-top" memo, which defines management's leadership and commitment towards an effective internal control structure.

The second tier is supported by the Internal Control team, consisting of subject matter experts providing guidance and execution of the program throughout the agency. The third tier is supported by the AUMs who manage at the program/directorate level within the organization. Each directorate's senior leadership, within each assessable unit, collaborates with AUMs to identify areas of risks in their respective area. The processes of coordinating and consolidating risk help identify the overall assessment of risk at the enterprise risk management level, while also reviewing DISA's detail transactions. This risk assessment results in reviews and letters of assurance from each area that are considered in the annual Statement of Assurance assessment.

***Oversight and Monitoring:***

DISA's internal control structure of training provides AUM assistance; ELCs; risk assessments; continuous testing in mandatory and high-risk areas; reviews, updates, and management approval of process narratives and cycle-memos; CAPs; and senior accountable officials (SOAs) letters of assurance. These elements are all core to an integral program of oversight and monitoring. In addition, the Senior Assessment Team (SAT) met on Sept. 27, 2023, and provided oversight to the internal control program through discussion of results and anticipated outcomes to be reported in the FY 2023 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.

***Financial Risk Management (FRM):***

One of the new recommendations for FY 2023 is the submission of the FRM or tone-at-the-top RMIC memorandum to the RMIC platform. This is a new submission item added in FY 2023 that is recommended, but not required. Components that do not have a tone-at-the-top memorandum that includes a commitment to combatting fraud, are encouraged to begin development.

***Risk Assessment Template:***

One of the new recommendations for FY 2023. Components that utilize emerging technologies should leverage the GAO AI framework as described in Government Accountability Office report GAO-21-519SP, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities". Components should consider risks around implementation of emerging technologies in their risk assessment.

***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.

***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 2023. 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 2023, 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 2023, 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 2022 and 2023.

***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 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 2023, DISA director signed a “tone-at-the-top” memo that defines management’s leadership and commitment towards an effective RMIC: openness, honesty, integrity, and ethical behavior. The memo directed the agency to follow a risk-based and results-oriented program in alignment with the GAO Green Book and OMB A-123. The tone-at-the top is set

throughout DISA by all levels of management and has a trickle-down effect on all employees.

The second tier is supported by a subject matter expert (SME) team. The team coordinates requirements with the OUSD comptroller regarding the RMIC Program, in addition to providing training, guidance, oversight, and review in accordance with directives to the AUMs. DISA provided internal control kick-off training for the AUMs in November 2022 and conducted three additional workshops in the FY 2023 reporting cycle to address risk assessments, testing grids, and letters of assurance. The RMIC team compiles assessable unit (AU) submissions for the agency's Statement of Assurance, facilitates information sharing between AUMs, consolidates results, and communicates outcomes to OUSD and agency leadership.

### ***Identification of Material Assessable Units***

The third tier is supported by the AUMs, who manage at the program/directorate level within the organization. For this reporting cycle, DISA identified 14 AUs:

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

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

### ***Identifying Key Controls***

Mandatory testing for all organizations is required to identify the functions performed within their area, in addition to the required testing areas of the Defense Travel System (DTS); Time and Attendance; and property, plant, and equipment (PP&E) to identify the level of process documentation available and determine the associated risk of those functions. Additionally, AUMs are responsible for identifying and documenting the key controls within their AUs in accordance with DOD Instruction 5010.40. The internal control team documents processes and key controls for all ICOR-FR functions through detailed cycle memoranda and narratives. Each AU documents its key processes and risks on the Risk Assessment Template. The OCFO RMIC team advises the AUMs to test, at a minimum, those key processes that were self-identified as high risk, as well as safety, security (if applicable), and the required testing areas. In addition, a checklist for records management was prepared by each AUM.

Each AU performs a risk assessment considering what is important to each area, such as those processes

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

### ***Developing the Test Plan/Executing the Test***

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

### ***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.

### ***Snapshot in Review***

#### ***Internal Controls Over Reporting - Operations***

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

#### ***Internal Controls Over Reporting - Financial Systems***

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

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

Additionally, DISA provides application hosting services for the department's service providers: the Defense Finance and Accounting Service (DFAS), the Defense Logistics Agency (DLA), the Defense Contract Management Agency (DCMA), the Defense Human Resource Activity (DHRA), military services, and other defense organizations. As a result, DISA is responsible for most of the general IT controls over the computing environment in which many financial, personnel, and logistics applications reside. For service providers and components to rely on automated controls and documentation within these applications, controls must be appropriately and effectively designed.

#### ***Internal Controls Over Reporting - Financial Reporting***

The OCFO documented end-to-end business processes and identified key internal control activities



supporting key business processes for ICOR-FR. DISA conducted an internal risk assessment that evaluated the results of prior year audits, internal analyses of the results of financial operations, and known upcoming business events. An internal control assessment was conducted within DISA for key mission-specific processes. The internal control team annually reviews and updates narratives and cycle memos of key processes. The internal control team maintains a Control Evaluation Matrix, which provides a detailed analysis, documents the Control Activities identified in the narratives, and includes mapping to a Financial Improvement and Audit Readiness (FIAR) Financial Reporting Objective; FIAR Risk of Material Misstatement, Test of Design and Implementation Effectiveness details; and test of Operating Effectiveness details.

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

**Figure 17-Areas of Testing**

General Fund	Working Capital Fund	Other
Data Quality Plan	CS Trial Balance (Rollforward) Testing	Active Users
Dormant Reviews	TSEAS Trial Balance (Rollforward) Testing	Departed Users
Year End Obligations	TSEAS Revenue	PP&E White House Communications Agency (WHCA) Existence and Completeness Training
Trial Balance Rollforward Testing	TSEAS Expenditure	Continuity of Operations Plan (COOP) Testing
GF Revenue	System Interface Agreement (SIA)	
GF Expenditure	CS Revenue	
CARES Act Testing	CS Expenditure	

The OUSD FIAR Office led department-wide discussions regarding SSAE 18 reviews and the impact to component financial statements. DISA identified more than 199 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 199 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 2023 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)
- Operations & Infrastructure Center (OPIC)
- Digital Capabilities and Security Center (DCSC)
- Chief of Staff (DDC)
- Inspector General (IG)
- Joint Force Headquarters DODIN (JFHQ-DODIN)
- Joint Service Provider (JSP)
- Hosting and Compute Center (HACC)
- White House Situation Room (WHSR)
- Procurement Services Directorate (PSD)
- Enterprise Integration and Innovation Center (EIIC)
- Operations & Infrastructure Center (OPIC)
- White House Communications Agency (WHCA)
- Workforce Services and Development Directorate (WSD)

**List of all Component material AUs related to ICOR**

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

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

**Figure 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 2023, 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, FY 2023 activities/goals include performing a technology refresh of the FAMIS software; implementing a compliant G-invoicing solution; completing Phase II of Direct Treasury Disbursing; implementing SOA/Web Services capabilities; and laying the groundwork to migrate FAMIS to a commercial cloud environment. In addition to the accounting system, DISA's financial systems environment is complemented by a select group of integrated financial tools and capabilities. These include:

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

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

In that regard, DISA is driving standardization of the customer order provisioning process to include a single integrated order entry solution for all orders while validating the solutions that integrate with DISA's financial and contracting systems and tools. DISA's financial systems strategy is purpose driven to continually innovate and increase its use of technologies, such as robotic process automation and artificial intelligence, to improve and automate financial and contractual transactions. As a result of DISA's experience using its newly modernized/compliant accounting systems for the previous three years, its accounting operations have stabilized, and it is taking advantage of its capabilities to improve accounting processes and audit readiness, and to set the course for further financial modernization efforts across its business ecosystem. This includes identifying and assessing opportunities to sunset older legacy supporting systems by consolidating and/or migrating functionality to more modern and flexible technologies and architectures.

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

#### 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 also anticipates continuation of partnerships with other federal agencies. The DOD/Veterans Affairs Integrated Electronic Health Record agreement to host all medical records in DISA data centers and the requirement for DOD to provide Public Key Infrastructure services to other federal agencies on a reimbursable basis are examples. 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 convergency 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.
- The enterprise-wide roll-out of a Cloud-Based Internet Isolation capability that isolates malicious code and content from DOD networks.

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

**Defense Information Systems Agency  
Working Capital Fund  
Principal Statements  
Fiscal Year 2023, Ending Sept. 30, 2023**

**Department of Defense**  
**Defense Information Systems Agency WCF**  
**As of Sept. 30, 2023 and 2022**  
**(\$ in thousands)**

**Figure 20-Balance Sheet**

	<u>2023</u>	<u>2022</u>
<b>Intragovernmental assets:</b>		
Fund Balance with Treasury (Note 2)	\$ 305,143	\$ 338,218
Accounts receivable, Net (Note 3)	872,973	735,901
Total Intragovernmental Assets	<u>1,178,116</u>	<u>1,074,119</u>
<b>Other than intragovernmental assets:</b>		
Accounts receivable, net (Note 3)	875	947
General property, plant and equipment, net (Note 4)	1,011,565	1,015,572
Advances and prepayments	0	257
Total other than intragovernmental assets	<u>1,012,440</u>	<u>1,016,776</u>
<b>Total Assets</b>	<u>\$ 2,190,556</u>	<u>\$ 2,090,895</u>
<b>Liabilities (Note 7)</b>		
<b>Intragovernmental liabilities:</b>		
Accounts payable	\$ 46,138	\$ 37,920
Advances from others and Deferred Revenue (Note 7)	0	257
Other Liabilities (Notes 7 and 9)	2,738	2,746
Total intragovernmental liabilities	<u>48,876</u>	<u>40,923</u>
<b>Other than intragovernmental liabilities:</b>		
Accounts payable	907,244	894,830
Federal employee benefits payable (Note 6)	5,276	4,376
Advances from others and Deferred Revenue (Note 7)	2	59
Other Liabilities (Notes 7, 8 and 9)	47,088	45,766
Total other than intragovernmental liabilities	<u>959,610</u>	<u>945,031</u>
<b>Total liabilities</b>	<u>1,008,486</u>	<u>985,954</u>
<b>Commitments and contingencies (Note 9)</b>		
<b>Net Position:</b>		
Cumulative Results from Operations	1,182,070	1,104,941
Total Cumulative Results of Operations (Consolidated)	<u>1,182,070</u>	<u>1,104,941</u>
Total net position	<u>1,182,070</u>	<u>1,104,941</u>
<b>Total liabilities and net position</b>	<u>\$ 2,190,556</u>	<u>\$ 2,090,895</u>

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

**Department of Defense  
 Defense Information Systems Agency WCF  
 For the Years Ended Sept. 30, 2023 and 2022  
 (\$ in thousands)**

**Figure 21-Statement of Net Cost**

<b>Gross Program Costs (Note 10, Note 13)</b>	<b>2023</b>	<b>2022</b>
Gross Costs (Note 10)	\$ 8,063,925	\$ 7,899,437
Less: Earned Revenue (Note 11)	(7,996,143)	(7,808,452)
<b>Net Cost of Operations</b>	<b>67,782</b>	<b>90,985</b>

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

**Department of Defense  
 Defense Information Systems Agency WCF  
 For the Years Ended Sept. 30, 2023 and 2022  
 (\$ in thousands)**

**Figure 22-Statement of Changes in Net Position**

<b>CUMULATIVE RESULTS OF OPERATIONS</b>	<b><u>2023</u></b>	<b><u>2022</u></b>
Beginning Balance	\$ 1,104,941	\$ 973,913
Non-exchange revenue	2	0
Transfers-in/out without reimbursement	109,458	198,938
Imputed financing	35,453	23,075
Other	(2)	(0)
Net Cost of Operations	67,782	90,985
Net Change in Cumulative Results of Operations	77,129	131,028
<b>Total Cumulative Results of Operation</b>	<b>1,182,070</b>	<b>1,104,941</b>
<b>Net Position</b>	<b>\$ 1,182,070</b>	<b>\$1,104,941</b>

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



**Department of Defense  
 Defense Information Systems Agency WCF  
 For the Years Ended Sept. 30, 2023 and 2022  
 (\$ in thousands)**

**Figure 23-Statement of Budgetary Resources**

	<u>2023</u>	<u>2022</u>
<b>Budgetary Resources</b>		
Unobligated balance from prior year budget authority, Net (Note 12)	\$ 107,808	\$ 98,506
Contract Authority (discretionary and mandatory)	113,040	188,081
Spending Authority from offsetting collections (discretionary and mandatory)	8,193,116	7,360,290
Total Budgetary Resources	<u>8,413,964</u>	<u>7,646,877</u>
<b>Status of Budgetary Resources</b>		
New obligations and upward adjustments (total)	8,043,398	7,539,069
Unobligated balance, end of year		
Apportioned, unexpired accounts	370,566	107,808
Unexpired unobligated balance, end of year	<u>370,566</u>	<u>107,808</u>
Unobligated balance, end of year (total)	<u>370,566</u>	<u>107,808</u>
Total Budgetary Resources	<u>8,413,964</u>	<u>7,646,877</u>
<b>Outlays, Net</b>		
Outlays, net (total) (discretionary and mandatory) (Note 13)	<u>33,075</u>	<u>(124,564)</u>
Agency Outlays, net (discretionary and mandatory)	<u>\$ 33,075</u>	<u>\$ (124,564)</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 2023, Ending Sept. 30, 2023**

**DEFENSE INFORMATION SYSTEMS AGENCY**  
**WORKING CAPITAL FUND**

**Notes to the Principal Statements**

**Fiscal Year 2023, Ending Sept. 30, 2023**

**Note 1. 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 comprise the department's reporting entity for the purposes of these financial statements.

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

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

### **1C. Fund Balance with Treasury**

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

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

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

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

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

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

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

For additional information, see *Fund Balance with Treasury Note 2* below.

#### **1D. Revenue and Other Financing Sources**

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

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

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

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

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

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

## 1E. Budgetary Terms

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

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

The following budgetary terms are commonly used:

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

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

## 1F. Changes in Entity or Financial Reporting

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.

## **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 \$370.6 million represents the cumulative amount of budgetary authority set aside to cover future obligations and is not restricted for future use. The available balance consists primarily of the unexpired, unobligated balance that has been apportioned and available for new obligations.

Obligated balance not yet disbursed in the amount of \$1.7 billion represents funds obligated for goods and services but not paid.

The Non-FBWT budgetary accounts in the amount of \$1.7 billion reduce budgetary resources and are primarily composed of unfilled customer orders without advance from customers in the amount of \$871.6 million, contract authority in the amount of \$174.3 million, and receivables and other in the amount of \$679.4 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>2023</u>	<u>2022</u>
Unobligated Balance:		
Available	\$ 370,566	\$ 107,808
<b>Total Unobligated Balance</b>	370,566	107,808
<b>Obligated Balance not yet Disbursed</b>	1,659,920	1,524,266
Non-FBWT Budgetary Accounts:		
Unfilled Customer Orders without Advance	(871,605)	(523,890)
Contract Authority	(174,314)	(226,977)
Receivables and Other	(679,424)	(542,989)
<b>Total Non-FBWT Budgetary Accounts</b>	(1,725,343)	(1,293,856)
<b>Total FBWT</b>	\$ 305,143	\$ 338,218

**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)

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

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

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

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

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

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	CY	PY
General PP&E, Net beginning of year	\$ 1,015,572	\$ 908,288
Capitalized Acquisitions	159,982	156,961
Dispositions	(11,513)	(6,223)
Transfers in/(out) without reimbursement	109,457	198,907
Depreciation Expense	(261,933)	(242,360)
<b>Balance at end of year</b>	<b>\$ 1,011,565</b>	<b>\$ 1,015,573</b>

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**

(thousands)

DISA WCF 2023 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
Leasehold Improvements	S/L	Lease term	\$ 0	\$ (0)	\$ 0
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
Construction-in-Progress	N/A	N/A	74,457	N/A	74,457
<b>Total General PP&amp;E</b>			<b>\$ 3,214,629</b>	<b>\$ (2,203,063)</b>	<b>\$ 1,011,565</b>

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

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

\*TSEAS uses 5 years for depreciation and CS uses 3 years for most depreciation, unless otherwise specified (10/20 years)

### Note 5. Liabilities Not Covered by Budgetary Resources

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

Intragovernmental liabilities-other comprise DISA WCF's unfunded Federal Employees' Compensation Act (FECA) liability in the amount of \$853 thousand. These liabilities will be funded in future periods.

Other than intragovernmental liabilities-federal employee benefits payable consist of various employee actuarial liabilities not due and payable during the current fiscal year. As of Sept. 30, 2023, DISA WCF's liabilities consist of actuarial FECA liability for workers' compensation benefits in the amount of \$4.9 million. These liabilities will be funded in future periods.

**Figure 28-Liabilities Not Covered by Budgetary Resources**

(thousands)		
DISA WCF	<u>2023</u>	<u>2022</u>
Intragovernmental Liabilities		
Other	\$ 853	\$ 948
<b>Total Intragovernmental Liabilities</b>	853	948
Other than Intragovernmental Liabilities		
Federal employee benefits payable	4,941	4,056
<b>Total Other than Intragovernmental Liabilities</b>	4,941	4,056
<b>Total Liabilities Not Covered by Budgetary Resources</b>	5,794	5,004
<b>Total Liabilities Covered by Budgetary Resources</b>	1,002,692	980,950
<b>Total Liabilities</b>	\$ 1,008,486	\$ 985,954

**Note 6. Federal Employee Benefits Payable**

Expense Components

For FY 2023, 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 \$9.4 million in total, of which \$4.9 million was distributed to DISA WCF based upon staffing ratios. DISA made the distribution using DISA's normal methodology of apportioning FECA liability to WCF based upon relative staffing levels. DISA used the same apportionment methodology in prior years.

Changes in Actuarial Liability

Fluctuations in the total liability amount charged to DISA by DOL will cause changes in FECA liability. FECA liability, which falls under other actuarial benefits, decreased \$884.1 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-Federal Employee Benefits Payable**

(thousands)

<b>DISA WCF 2023</b>	<b>Liabilities</b>	<b>(Assets Available to Pay Benefits)</b>	<b>Unfunded Liabilities</b>
Other Benefits			
FECA	\$ 4,941	\$ (0)	\$ 4,941
Other	335	(335)	0
<b>Total Other Benefits</b>	<b>5,276</b>	<b>(335)</b>	<b>4,941</b>
<b>Federal Employee Benefits Payable</b>	<b>5,276</b>	<b>(335)</b>	<b>4,941</b>
Other benefit-related payables included in Intragovernmental Other Liabilities	2,737	(1,884)	853
<b>Total Federal Employee Benefits Payable</b>	<b>\$ 8,013</b>	<b>\$ (2,219)</b>	<b>\$ 5,794</b>

<b>DISA WCF 2022</b>	<b>Liabilities</b>	<b>(Assets Available to Pay Benefits)</b>	<b>Unfunded Liabilities</b>
Other Benefits			
FECA	\$ 4,056	\$ (0)	\$ 4,056
Other	319	(319)	0
<b>Total Other Benefits</b>	<b>4,375</b>	<b>(319)</b>	<b>4,056</b>
<b>Federal Employee Benefits Payable</b>	<b>4,375</b>	<b>(319)</b>	<b>4,056</b>
Other benefit-related payables included in Intragovernmental Other Liabilities	2,746	(1,798)	948
<b>Total Federal Employee Benefits Payable</b>	<b>\$ 7,121</b>	<b>\$ (2,117)</b>	<b>\$ 5,004</b>

**Note 7. Other Liabilities**

**Other Than Intragovernmental**

Accrued funded payroll and benefits: \$47.1 million. DISA WCF reports the unpaid portion of accrued funded civilian payroll and employees' annual leave as it is earned as other liabilities, and subsequently reduces the leave liability when it is used. Unused leave is an unfunded liability, which will be paid from future resources when taken or when the employee retires or separates. The liability reported at the end of the accounting period reflects the current pay rates. When sick leave is earned, a liability is not recognized for unused amounts because employees do not vest in this benefit. Sick and holiday leave is expensed when taken.

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 2023	Current Liability	Non-Current Liability	Total
<b>Intragovernmental</b>			
Liabilities for Non-entity Assets	\$ 2	\$ 0	\$ 2
Other Liabilities	0	0	0
Subtotal	2	0	2
Other Liabilities	2,251	486	2,737
<b>Total Intragovernmental</b>	2,252	486	2,738
Other than Intragovernmental			
Accrued Funded Payroll and Benefits	47,088	0	47,088
<b>Total Other than Intragovernmental</b>	47,088	0	47,088
<b>Total Other Liabilities</b>	\$ 49,340	\$ 486	\$ 49,826

DISA WCF 2022	Current Liability	Non-Current Liability	Total
<b>Intragovernmental</b>			
Liabilities for Non-entity Assets	\$ 0	\$ 0	\$ 0
Other Liabilities	0	0	0
Subtotal	0	0	0
Other Liabilities	2,294	452	2,746
<b>Total Intragovernmental</b>	2,294	452	2,746
Other than Intragovernmental			
Accrued Funded Payroll and Benefits	45,766	0	45,766
<b>Total Other than Intragovernmental</b>	45,766	0	45,766
<b>Total Other Liabilities</b>	\$ 48,060	\$ 452	\$ 48,512

**Note 8. Leases****Figure 31-Entity as Lessee - Assets Under Capital Lease (Table 16A)**

(thousands)

DISA WCF	2023	2022
Equipment	\$ 332,784	\$ 316,863
Accumulated Amortization	(270,665)	(261,502)
<b>Total Capital Lease</b>	\$ 62,119	\$ 55,361

DISA WCF records assets that meet the capital lease criteria defined by FASAB SFFAS 6. These assets represent agreements for the exclusive use of certain transoceanic cables in support of network communications as part of the optical transport network. All DISA WCF capital leases are considered Non-Federal.

In prior fiscal years, DISA WCF transferred in Defense Information Systems Network Core Program capital leases and accumulated amortization from DISA General Fund (GF). DISA paid for these leases in full at inception. While this does not create a liability, a prepaid rent asset is created that will be used to

reduce future rent liabilities as they become due.

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

DISA WCF has operating leases for land, buildings, and equipment. Future lease payments due as of Sept. 30, 2023, for non-cancelable operating leases were as follows:

**Figure 32-Future Payments Due for Non-Cancelable Operating Leases (Table 16D)**

(thousands)

DISA WCF 2023	Land & Buildings	Equipment	Total
Federal			
Fiscal Year 2024	\$ 732	\$ 425	\$ 1,157
Fiscal Year 2025	756	395	1,151
Fiscal Year 2026	780	395	1,175
Fiscal Year 2027	804	395	1,199
Fiscal Year 2028	266	33	299
<b>Total Federal Future Lease Payments</b>	<b>3,338</b>	<b>1,643</b>	<b>4,981</b>
<b>Total Non-Federal Future Lease Payments</b>	<b>0</b>	<b>0</b>	<b>0</b>
<b>Total Future Lease Payments</b>	<b>\$ 3,338</b>	<b>\$ 1,643</b>	<b>\$ 4,981</b>

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

Land and Building Leases

As of Sept. 30, 2023, 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 federal. This lease generally requires DISA WCF to pay property taxes, utilities, security, custodial services, parking, and operating expenses. Certain leases contain renewal options.

Equipment Leases

Equipment leases are operating leases for photocopiers and vehicles. DISA WCF currently leases 133 photocopiers and 21 vehicles located across various sites. The photocopiers are leased for three years, while the vehicles are leased for one year with annual renewal options.

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

**Note 9. Commitments and Contingencies**

DISA WCF may be a party in various administrative proceedings and legal actions related to claims for environmental damage, equal opportunity matters, and contractual bid protests. DISA WCF reviews the agency claims report and determines if a liability should be recorded for the reporting period. DISA WCF did not record any contingent liabilities for the fourth quarter of FY 2023 reporting.

**Note 10. Suborganization Program Costs**

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

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

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

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

**Figure 33-Statement of Net Cost by Responsibility Segment Cost and Earned Revenues with the Public and Intragovernmental Entities**

(thousands)				
Lines of Business	With the Public	Intragovernmental	Intra-WCF Eliminations	FY 2023
<b>Computing Services</b>				
Gross Costs	\$ (801)	\$ (6,755)	\$ 0	\$ (7,556)
Less earned revenues	(503)	(19)	0	(522)
Net Costs	(1,304)	(6,774)	0	(8,078)
<b>TSEAS</b>				
Gross Costs	7,804,112	301,523	0	8,105,635
Less earned revenues	(1,357)	(7,994,264)	0	(7,995,621)
Net Costs	7,802,755	(7,692,741)	0	110,014
<b>Component Level</b>				
Gross Costs	0	0	(34,154)	(34,154)
Less earned revenues	0	0	0	0
Net Costs	0	0	(34,154)	(34,154)
<b>Net Cost of Operations</b>				
Gross Costs	7,803,311	294,768	(34,154)	8,063,925
Less Total Revenues	(1,860)	(7,994,283)	0	(7,996,143)
Total Net Costs	\$ 7,801,451	\$ (7,699,515)	\$ (34,154)	\$ 67,782

Lines of Business	With the Public	Intragovernmental	Intra-WCF Eliminations	FY 2022
<b>Computing Services</b>				
Gross Costs	\$ (15,823)	\$ 31,309	\$ 0	\$ 15,486
Less earned revenues	7	(78,484)	0	(78,477)
Net Costs	(15,817)	(47,175)	0	(62,991)
<b>TSEAS</b>				
Gross Costs	7,681,192	247,492	0	7,928,683
Less earned revenues	(1,150)	(7,740,688)	0	(7,741,838)
Net Costs	7,680,042	(7,493,197)	0	186,845
<b>Component Level</b>				
Gross Costs	(170,813)	170,813	(44,733)	(44,733)
Less earned revenues	0	0	11,864	11,864
Net Costs	(170,813)	170,813	(32,869)	(32,869)
<b>Net Cost of Operations</b>				
Gross Costs	7,494,556	449,614	(44,733)	7,899,437
Less Total Revenues	(1,143)	(7,819,172)	11,864	(7,808,452)
Total Net Costs	\$ 7,493,413	\$ (7,369,559)	\$ (32,869)	\$ 90,985

\*Prior year component level represents adjustments entered into the Defense Departmental Reporting System (DDRS) at the DISA consolidated level.

### Note 11. Exchange Revenues

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

### Note 12. 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, 2023, DISA WCF incurred \$8 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, 2023, is \$370.6 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, 2023, DISA WCF’s net amount of budgetary resources obligated for undelivered orders is \$853.5 million.

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

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

**Figure 34-Budgetary Resources Obligated for Undelivered Orders at the End of the Period**

		(thousands)	
<b>DISA WCF</b>		<b>2023</b>	<b>2022</b>
Intragovernmental			
Unpaid		\$ 38,109	\$ 28,765
<b>Total Intragovernmental</b>		38,109	28,765
Non-Federal			
Unpaid		815,401	711,146
Prepaid/Advanced			257
<b>Total Non-Federal</b>		815,401	711,403
<b>Total Budgetary Resources Obligated for Undelivered Orders at the End of the Period</b>		\$ 853,510	\$ 740,168

**Note 13. 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 35- Reconciliation of the Net Cost of Operations to Net Outlays**

(thousands)			
DISA WCF 2023	Intragovernmental	With the Public	Total
<b>Net Cost of Operations (SNC)</b>	\$ (7,708,698)	\$ 7,776,480	\$ 67,782
<b>Components of Net Cost Not Part of Net Outlays:</b>			
Property, plant, and equipment, net changes	0	(4,007)	(4,007)
Increase/(decrease) in assets:			
Accounts and taxes receivable, net	137,071	(72)	136,999
Other assets	0	(257)	(257)
(Increase)/decrease in liabilities:			
Accounts Payable	(8,219)	(12,412)	(20,631)
Federal employee benefits payable	0	(900)	(900)
Other liabilities	265	(1,265)	(1,000)
Other financing sources:			
Imputed cost	(35,453)	0	(35,453)
<b>Total Components of Net Cost That are Not Part of Net Outlays</b>	93,664	(18,913)	74,751
<b>Miscellaneous Reconciling Items</b>			
<b>Total Other Reconciling Items</b>	(109,458)	0	(109,458)
<b>Total Net Outlays</b>	\$ (7,724,492)	\$ 7,757,567	\$ 33,075
<b>Agency Outlays, Net, Statement of Budgetary Resources</b>			33,075
<b>Unreconciled difference</b>			\$ 0

**Defense Information Systems Agency  
Working Capital Fund  
Required Supplementary Information  
Fiscal Year 2023, Ending Sept. 30, 2023**

## **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 2023 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 2023, all real property has been transferred out of the DISA WCF.

For FY 2023, deferred maintenance reporting continues to be reviewed and revised as needed. The WCF does not have DM&R related to capitalized general PP&E, stewardship PP&E, non-capitalized or fully depreciated general PP&E. In addition, the DISA WCF does not have PP&E for which management does not measure and/or report DM&R. The rationale for excluding any PP&E asset other than if not capitalized or it is fully depreciated, is the item does not meet the applicable capitalization criteria, is not on the integrated project list, or there are preventative maintenance contracts in place to address maintenance needs in the current year.

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

**Defense Information Systems Agency**  
**Working Capital Fund**  
**As of Sept. 30, 2023**  
**(thousands)**

**Figure 36-Combining Statement of Budgetary Resources**

	<b>CS</b>	<b>TSEAS</b>	<b>FY 2023</b>
<b>Budgetary Resources (discretionary and mandatory):</b>			
Unobligated balance from prior year budget authority, net	\$ 786,711	\$ (678,903)	\$ 107,808
Contract Authority (discretionary and mandatory)	(39,576)	152,616	113,040
Spending Authority from offsetting collections	(14,162)	8,207,278	8,193,116
<b>Total Budgetary Resources</b>	<b>732,973</b>	<b>7,680,991</b>	<b>8,413,964</b>
<b>Status of Budgetary Resources:</b>			
New obligations and upward adjustments (total)	(46,801)	8,090,199	8,043,398
Unobligated balance, end of year: Apportioned, unexpired accounts	0	370,566	370,566
Unobligated balance, end of year: Unapportioned, unexpired accounts	779,774	(779,774)	0
Unexpired unobligated balance, end of year	779,774	(409,208)	370,566
Unobligated balance, end of year (total)	779,774	(409,208)	370,566
<b>Total Budgetary Resources</b>	<b>732,973</b>	<b>7,680,991</b>	<b>8,413,964</b>
<b>Outlays, net:</b>			
Outlays, net (total) (discretionary and mandatory)	6,607	26,468	33,075
Agency Outlays, net (discretionary and mandatory)	\$ 6,607	\$ 26,468	\$ 33,075

**Defense Information Systems Agency  
Working Capital Fund  
Other Information  
Fiscal Year 2023, Ending Sept. 30, 2023**

**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	5	0	0	2	3
PPE	1	0	1	0	0
<b>Total Material Weaknesses</b>	<b>6</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>

**Figure 38-Effectiveness of Internal Control over Financial Reporting (FMFIA§ 2)**

**Statement of Assurance:** Unmodified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Fund Balance with Treasury	5	0	0	1	1	3
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	1	0	1	0	0	0
<b>Total Material Weaknesses</b>	<b>6</b>	<b>0</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>3</b>

**Figure 39-Effectiveness of Internal Control over Operations (FMFIA§ 2)**

**Statement of Assurance:** Unmodified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
<b>Total Material Weaknesses</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

**Figure 40- 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
<b>Total non-conformance</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

**Figure 41-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 except as noted in fund balance with treasury related material weaknesses above	No lack of compliance noted



## Management Challenges



19-Oct-2023

MEMORANDUM FOR DIRECTOR (D)

SUBJECT: Top Management and Performance Challenges Facing the Defense Information Systems Agency (DISA) in Fiscal Year 2024

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 2024.

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. In addition, we recognize that DISA faces the extraordinary task of meeting these challenges while working in a hybrid work environment.

The DISA OIG identified seven 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 2024 include:

- Meeting Data Management Challenges
- Managing Human Capital
- Cyber Supply Chain
- Current and Future Contracting Environment
- Mission Partner Payments
- Artificial Intelligence
- Safeguarding and Handling Classified Information

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

Stephen M. Ryan  
Inspector General

# Challenge 1

## Meeting Data Management Challenges

---

Data management is the practice of collecting, keeping, and using data securely. DISA transports mission partner data internally and externally while maintaining various operating systems that produce massive amounts of complex data.

The federal government, Department of Defense (DoD), and DISA, are under constant data-driven cyber-attacks. For example, the Federal Bureau of Investigations (FBI), National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency (CISA) announced that hostile state-sponsored hackers targeted and breached U.S. defense and industry critical infrastructure.

To help address these challenges, DoD outlined data management goals in the 2020 DoD Data Strategy. Per the Strategy, DoD aims to protect data and evolve data into actionable information for decision makers. The DoD Data Strategy describes the DoD vision, guiding principles, essential capabilities, and goals for data management throughout the DoD.

DISA has the responsibility to help DoD modernize the infrastructure and identify, protect, detect, respond, and recover from data threats. The DISA Office of the Chief Data Officer (OCDO) was formally established in the standing up of Enterprise Integration and Innovation (EII) in September 2021. In 2022, the CDO published the DISA Data Strategy Implementation Plan (IPlan) to describe a modern approach to information architecture and data management, outline workstreams necessary to organize activities, define future activities, and identify next steps for the DISA organization. The DISA IPlan aligns with the DoD Data Strategy, DISA Strategy, and expands upon DISA's efforts to meet DoD data management principles, capabilities, and goals. DISA also created the DISA Data Analytics Center of Excellence to bridge business policies, cyber, and information technology. In 2023, the DISA OIG is assessing DISA's data management maturity.

## Challenge 2

# Managing Human Capital

---

DISA workforce continues as a hybrid work environment with most employees having the option to work from home more frequently. Moving forward in the hybrid work environment, DISA leadership will continue to be presented with many challenges including maintaining employee morale and productivity, acquiring the necessary and relevant technology and tools, and recruiting and retaining talent.

Recruiting talent continues to be a challenge and recruiting individuals with the right talent in a timely manner is critical. 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 and provide a place talented individuals want to work. DISA competes for talent with the private sector, where additional benefits and flexibilities can be used to recruit highly qualified workers. DISA's telework and remote work policies allow leadership to broaden the hiring pool of candidates in various geographical regions to attract and retain high quality talent. However, leadership will have to balance the use of telework and remote work to ensure mission requirements are met while providing the flexibilities to recruit and retain a skilled cyber workforce.

As DISA continues to strengthen the work culture, the agency invests in key initiatives to attract and retain a talent pool skilled in critical thinking and diverse in ideas, backgrounds, and technical expertise. To achieve this, DISA is forecasting needed skills through succession planning, improving how it markets career opportunities within the agency, and deepening external partnerships with educational institutions and third-party personnel services.

*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 onboard 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.

## Challenge 3

# Cyber Supply Chain

---

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

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

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

In 2022, the DISA OIG conducted an evaluation of DISA's ICT-SCRM program and processes. The OIG observed DISA's ICT-SCRM program developed several best practices and the Agency has made significant program investments. For example, DISA created an ICT-SCRM management office, assigned an acting Branch Chief, and updated the Agency's ICT-SCRM instruction along with a Strategy and Implementation Plan. The DISA team has developed in-depth analysis and documentation of ICT suppliers and products. As a result, the DISA team is often sought after to support and train external agencies on ICT-SCRM activities. The creation of these operational relationships enhances DISA's capability to secure the DoD supply chain and support the Warfighter's ability to mitigate risk at the tactical level. Moving forward, DISA is focusing on ICT-SCRM related activities to address hardware bill of material (HBOM) rogue/counterfeit detection and software bill of material (SBOM) zero-day mitigation efforts.

Despite these positive elements, the OIG determined DISA can better define ICT-SCRM processes and provide additional operational guidance to increase the maturity of the program. We also found inconsistent ICT-SCRM performance across the agency, stakeholders lacked familiarity with ICT-SCRM, efforts were stove-piped, and training was not conducted in accordance with DISA requirements. The OIG identified the following four recommendations as part of our corrective action process: (1) Define, in writing, ICT-SCRM process steps,

integration with other corporate processes, and provide additional operational guidance in accordance with DISAI 240-110-44; (2) Develop DISA ICT-SCRM training in accordance with NIST SP 800-161 Rev 1 and DISAI 240-110-44 to ensure a common understanding of processes and methods throughout the organization; (3) Establish ICT-SCRM metrics and benchmarking for performance analysis; (4) Develop an oversight process to ensure DISA's ICT-SCRM repository maintains all required SCRM threats, vulnerabilities, and reporting; including Criticality Analysis, Due Diligence Reports, and Risk Assessment artifacts.

Since the realignment of the DISA ICT-SCRM program on 01 July 2023, the Risk Management Executive, Threat Mitigation Division (RE3), continues to focus on the development of foundational program requirements while maintaining program execution. Of the four OIG recommendations made in 2022, two have been satisfied through the creation of an internal ICT-SCRM SharePoint page and ticketing system. RE3 continues to address the outstanding DISA OIG recommendations by updating the ICT-SCRM CONOPs and the development of DISA ICT-SCRM annual training; both efforts are on track to be completed by the end of calendar year 2023 (CY23).

## **Challenge 4**

# **Current and Future Contracting Environment**

---

Contracting is a top management challenge at DISA due in part to resource constraints. The DISA Defense Information Technology Contracting Organization (DITCO) procures complex mission partner IT, Cyber, and Telecommunications requirements. The Office of Personnel Management has determined the 1102 (contracting) job series a critical hiring need for which there is a severe shortage of candidates. DITCO hires a disproportionate number of career ladder positions (e.g., hire a GS-11 with limited contracting skills for complex requirements and best value trade off source selections into GS-13 full performance level positions). This also creates increased work for more experienced 1102s to provide substantive on-the-job training, and causes an inability to sufficiently and effectively meet DoD and other federal agency mission needs. DITCO's mission is to provide efficient and compliant procurement services for Information Technology, Cyber, and Telecommunication services that support national defense partners through timely, quality, and ethical contracting. DITCO has turned away mission partner requests, resulting in lost revenue, due to DITCO's mission requirements, workload, and hiring challenges.

In addition, DITCO identified the submission of late procurement packages and late funding from internal and external mission partners as a systemic, significant challenge. Late procurement packages occurred because of lack of planning, contract package routing delays, requirement definition issues, incomplete and unactionable procurement packages, unfunded requirement delays, and contract scope issues. This and other challenges in contracting faced by DITCO and mission partners are increased by Office of Management and Budget (OMB), Office of the Secretary of Defense (OSD), DoD, and DISA funding levels, increased contract documentation, incrementally funding contracts in small increments throughout the fiscal year which creates exponentially more work across the Agency, and other indirect process requirements. Among these are inefficient contracting information systems and interfaces which creates a substantive amount of manual work (and/or re-work) to include: (1) IDEAS Telecommunications contract writing system with a significant backlog of system enhancements, as well as down-time due to technical challenges and inoperable features, (2) lack of a circuit Review and Revalidation capability, and (3) DoD Procure to Pay Handshakes (i.e., data transfer) interfaces. DITCO and the Office of the Chief Financial Officer continue to collaborate to implement process improvements to fulfill contract requirements in a timely manner and meet mission partner needs.

The DISA OIG reported concerns relating to contracting at DISA; specifically, contracts pertaining to Government-Furnished Property, cyber safeguards of defense information, Government Purchase Card oversight, timely contract closeout, and management of unliquidated obligations. Additionally, the OIG identified concerns relating to Contracting Officer's Representatives (CORs) performing their duties and DITCO's oversight of CORs. CORs ensure delivery of supplies and critical mission services; however, inadequate COR oversight could result in decreased quality of contractor services.

## **Challenge 5**

### **Mission Partner Payments**

---

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 2023, the DISA 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.

We determined that DISA was not consistently pursuing collection of \$137 million in aged Accounts Receivable (A/R) over 30 days from Mission Partners as of 30 June 2022, in accordance with the Department of Defense Financial Management Regulation (DoD FMR). DISA J8 did not pursue collections for General Fund (GF); however, J8 issued Working Capital Fund's (WCF's) collection Memorandums. We found internal control weaknesses, including incomplete policy, limited automated capabilities and processes, lack of compliance with the policy, and a policy that did not include the processes for classified and unbillable A/R transactions.

The audit also found DISA WCF was unable to bill Mission Partners for \$77 million aged A/R over 90 days as of June 2022. DISA was performing work without funding documentation including a Standard Line of Accounting (SLOA) because DISA did not require Mission Partners to provide the SLOA prior to performing work for reoccurring services. DISA does have recurring and automated communication with Mission Partners, requesting the SLOA; however, many Mission Partners were not responsive in providing the SLOA when requested. Additionally, DISA's policy did not include the process for obtaining Mission Partners funding documentation with a SLOA prior to DISA providing the services that are recurring in nature, crossing fiscal years..

Incomplete and limited automated capabilities to accomplish and carryout policy for the collection process hinders J8's ability to receive timely reimbursement for services and the lack of funding information leads to delays in Mission Partner payments for services provided. The DISA OIG made six recommendations to address these issues.

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 dictate and enforce a standard process across DISA.

## Challenge 6

# 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. Participants learned about various AI initiatives within DISA and around the Department of Defense. 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.



## Challenge 7

# Safeguarding and Handling Classified Information

---

Safeguarding sensitive and classified data is a top management challenge to DISA, not only for the organization but also for mission partners. DISA provides crucial infrastructure and network capabilities enabling DoD Organizations and our global partners with carrying out strategic objectives as well as their daily business operations. Internal controls and security of sensitive information is not only a national defense priority, it comes with a significant cost to maintain.

In April 2023, the DoD CIO issued a memorandum “*Department of Defense Guidance on Safeguarding Responsibilities Regarding Classified Information*” regarding the improvement of controls around safeguarding classified information. In response, DISA leadership took action by issuing Operations Orders to address unauthorized disclosures and report postures and actions taken to improve compliance.

Recent DoD incidents relating to military service members, personnel, and contractors accessing and distributing sensitive and classified data have occurred from reasons such as personal ethics to espionage by nation states. These increasing number of incidents within DoD raise concerns by senior leadership over DoD’s organizational and personnel access to sensitive infrastructure and data, what requirements are there to access data, and what systems are connected to this sensitive infrastructure. The resulting fallout from spillage or unauthorized disclosure incidents not only damages National Security, but also could threaten DISA’s strategic mission, DISA’s reputation within the DoD, and the loss of trust with our mission partners.

## OFFICE OF THE INSPECTOR GENERAL

The Office of the Inspector General (OIG) is an impartial fact-finder for the director and leaders of DISA. The OIG seeks to improve the efficiency and effectiveness of DISA's programs and operations by conducting [audits](#), [investigations](#), and [evaluations](#). The OIG then evaluates and coordinates to close the recommendations through the [Liaison](#) office.

### AUDIT

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

### INVESTIGATION

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

### EVALUATION

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

### LIAISON

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

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

## **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 2023.

**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

December 15, 2023

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 2023 and FY 2022

(Project No. D2023-D000FL-0057.000, Report No. DODIG-2024-038)

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, 2023, and 2022. 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 DISA'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, May 2023, Volume 2, May 2023, and Volume 3, June 2023. 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, 2023 and 2022, are presented fairly in all material respects, in accordance with Generally Accepted Accounting Principles.

Kearney's separate report, "Independent Auditor's Report on Internal Control over Financial Reporting," discusses one material weakness related to the DISA Working Capital Fund's internal controls over financial reporting. Specifically, Kearney's report

\* 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.

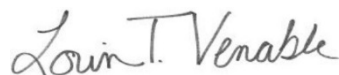
stated that DISA did not design or implement controls to reconcile and accurately report Fund Balance With Treasury.

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

In connect 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 2023 and FY 2022 Financial Statements and related notes. Furthermore, we do not express conclusions on the effectiveness of internal controls over financial reporting, on whether DISA's financial systems substantially complied with Federal Financial Management Improvement Act of 1996 requirements, or on compliance with provisions of applicable laws and regulations, contracts, and grant agreements. Our review disclosed no instances where Kearney did not comply, in all material respects, with GAGAS. Kearney is responsible for the attached December 15, 2023 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

# **Independent Auditor's Report**

## INDEPENDENT AUDITOR'S REPORT

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

### Report on the Audit of the Financial Statements

#### *Opinion*

We have audited the Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency (DISA), which comprise the Balance Sheets as of September 30, 2023 and 2022, 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, 2023 and 2022 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. 24-01, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of our report. We are required to be independent of DISA WCF and to meet our other ethical responsibilities in accordance with the relevant ethical requirements relating to our audits. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

#### *Responsibilities of Management for the Financial Statements*

Management is responsible for: 1) the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America; 2) the preparation, measurement, and presentation of Required Supplementary Information (RSI) in accordance with U.S. generally accepted accounting principles; 3) the preparation and presentation of Other Information included in DISA WCF's Agency Financial Report (AFR), as well as ensuring the consistency of that information with the audited financial statements and the RSI; and 4) the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.



In preparing the financial statements, management is required to evaluate whether there are conditions or events, considered in the aggregate, that raise substantial doubt about DISA WCF's ability to continue as a going concern for 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 *Government Auditing Standards* will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

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

- Exercise professional judgment and maintain professional skepticism throughout the audit
- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of DISA WCF's internal control. Accordingly, no such opinion is expressed
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements
- Conclude whether, in our judgment, there are conditions or events, considered in the aggregate, that raise substantial doubt about DISA WCF's ability to continue as a going concern for a reasonable period of time.

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

#### *Required Supplementary Information*

Accounting principles generally accepted in the United States of America require that Management's Discussion and Analysis and other RSI be presented to supplement the financial statements. Such information is the responsibility of management and, although not a part of the basic financial statements, is required by OMB and the Federal Accounting Standards Advisory Board (FASAB), who consider it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the RSI in accordance with *Government Auditing Standards*, 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 basic financial statements, and other knowledge we obtained during our audits of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

#### *Other Information*

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

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

#### **Other Reporting Required by *Government Auditing Standards***

In accordance with *Government Auditing Standards* and OMB Bulletin No. 24-01, we have also issued reports, dated December 15, 2023, on our consideration of DISA WCF's internal control over financial reporting and on our tests of DISA WCF's compliance with provisions of applicable laws, regulations, contracts, and grant agreements, as well as other matters for the year ended September 30, 2023. 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. 24-01 and should be considered in assessing the results of our audits.

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

Alexandria, Virginia  
December 15, 2023

## 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. 24-01, *Audit Requirements for Federal Financial Statements*, the Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency (DISA) as of and for the year ended September 30, 2023, and the related notes to the financial statements, which collectively comprise DISA WCF's basic financial statements, and we have issued our report thereon dated December 15, 2023.

### 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. 24-01. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA), such as those controls relevant to ensuring efficient operations.

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

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



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

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.

### **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 (AFR). DISA WCF concurred with the findings identified in our engagement. DISA WCF's response was not subjected to the other auditing procedures applied in the audit of the financial statements; accordingly, we express no opinion on the response.

### **Purpose of this Report**

The purpose of this report is solely to describe the scope of our testing of internal control and the results of that testing, and not to provide an opinion on the effectiveness of DISA WCF's internal control. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 24-01 in considering the entity's internal control. Accordingly, this report is not suitable for any other purpose.

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

Alexandria, Virginia  
December 15, 2023

## Schedule of Findings

### Material Weakness

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 material weakness presented in this Schedule of Findings has been formulated based on our determination of how individual control deficiencies, in aggregate, affect internal control over financial reporting. *Exhibit 1* presents the material weakness identified during our audit.

***Exhibit 1: Material Weakness and Sub-Categories***

Material Weakness	Material Weakness Sub-Category
I. Fund Balance with Treasury	A. Budget Clearing Account Reconciliation and Reporting Processes B. Statement of Differences Reconciliation and Reporting Processes

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

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

- A. Budget Clearing Account Reconciliation and Reporting Processes
- B. Statement of Differences Reconciliation and Reporting Processes

#### **A. Budget Clearing Account Reconciliation and Reporting Processes**

**Background:** DISA’s service organization manages, reports, and accounts for Fund Balance with Treasury (FBWT) budget clearing (suspense) account activities to the U.S. Department of the Treasury (Treasury). In addition to monitoring and approving the FBWT reconciliations performed by its service organization on its behalf, DISA 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 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, DISA'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 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 suspense transactions, if any, are included and accounted for in Treasury Index (TI)-97 Other Defense Organizations (ODO), Department of the Navy (TI-17), Department of the Air Force (TI-57), and Department of the Army (TI-21) suspense accounts based on DoD disbursing processes.

**Condition:** DISA, in coordination with its service organization, has not implemented sufficient internal control activities to ensure that transactions recorded in suspense accounts do not contain DISA collections and disbursements that should be recognized in the DISA accounting records. 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's service organization prepares quarterly suspense materiality assessments for each TI to identify the total count and amount of suspense account transactions resolved to DISA and other Defense agencies, the uncleared suspense transactions included in the assessment are material and the assessments are not available in a timely manner to perform sufficient analysis for financial reporting.

**Cause:** DISA's suspense activity is not recorded in unique suspense accounts, but rather in shared TI-97, TI-57, TI-21, and TI-17 suspense accounts. DoD suspense accounts continue to contain a high volume of collections and disbursements which require manual research and resolution. That manual research and resolution is what supports the production of the final UoTs and materiality assessments, but it 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 "to be determined" (TBD). As of FY 2023 Quarter (Q) 3, the following were noted as "TBD" in the suspense UoTs:

- TI-17 reported 14 out of 2,799 transactions (1%) totaling (\$1.3 million) net and \$1.3 million absolute (ABS) (11%)
- TI-21 reported 566 out of 2,380 transactions (24%) totaling (\$27.2 million) net and \$62.3 million ABS (12%)
- TI-57 reported 863 out of 1,380 transactions (63%) totaling \$9.5 million net and \$21.7 million ABS (45%)
- TI-97 reported 19,101 out of 19,618 transactions (97%) totaling \$(320.9 million) net and \$655.9 million ABS (97%).

DISA and its service organization have not designed and implemented a methodology to determine the financial reporting impact of DoD suspense account balances to DISA's financial

statements for financial reporting in a timely manner sufficient for quarterly and annual financial reporting timelines. The assessments do not identify amounts attributed to DISA 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's FBWT represents its claim to the Federal Government's resources and its accounts with Treasury for which DISA is authorized to make expenditures and pay liabilities. The materiality assessment methodology is not designed effectively as it pertains to recording an FBWT projection, should a material misstatement be identified. SFFAS No. 1 does not permit FBWT as a viable account for estimated amounts.

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

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

1. Continue implementing business process improvements in the related financial statement line items to prevent items from reaching suspense. Specifically, DISA should develop and implement monitoring controls and processes for Accounts Receivable (AR) and Accounts Payable (AP) balances to reduce the risk of DISA having a material amount of disbursements and collections not reflected on its financial statements.
2. Research and resolve suspense transactions by correcting the transactions in source systems and assist DISA's service organization with necessary supporting documentation for corrections, if needed.
3. Consider any limitations to DISA's service organization suspense account reconciliation process and develop compensating controls to reconcile any included FBWT suspense activity or, through documented materiality analysis, indicate that management accepts the risk of potential misstatement. This includes considering the materiality assessments and the amount of "TBD" data included, as well as the risk that DISA could have material transactions included in what is flagged as "TBD" in the UoTs that are used to create those assessments.
4. Pursuant to receiving the necessary information and documentation from DISA's service organization, develop and implement procedures to identify DISA's suspense account balances for recording and reporting into the GLs and financial statements.

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

1. Continue to develop procedures to determine what portion of the suspense balances, if



any, should be attributed to DISA for financial reporting in a timely manner and made available for year-end financial reporting purposes.

2. Continue to monitor and track the resolution of suspense activity cleared to DISA to enable 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. Continue to work to develop effective system and process controls to ensure that disbursements and collections are processed with valid TI, Treasury Account Symbol (TAS), and FY inputs.
4. Continue to develop and implement processes and controls to eliminate instances where transactions are being placed in suspense accounts intentionally.
5. Develop and implement a process to establish unique identifiers for each transaction in suspense UoTs that roll forward from period to period. DISA’s service organization should develop controls over the establishment and roll-over of those unique identifiers that can be tested for reliance.

## **B. Statement of Differences Reconciliation and Reporting Processes**

**Background:** DISA’s service organization provides daily Non-Treasury Disbursing Office (NTDO) disbursing services under various Agency Location Codes (ALC), often referred to as Disbursing Symbol Station Numbers (DSSN). Additionally, DISA’s service organization provides monthly Treasury reporting services under various reporting ALCs, which are different than disbursing ALCs. Monthly, NTDO disbursing activity is submitted to its assigned reporting ALC to generate a consolidated Standard Form (SF)-1219, *Statement of Accountability*, and SF-1220, *Statement of Transactions*. Daily, Treasury Disbursing Office (TDO) ALCs submit reports directly to Treasury and complete SF-224, *Statement of Transactions*, at month-end.

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’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 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.

**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. Assessments with fully cleared data identified to an entity are not available in a timely manner to perform sufficient analysis for financial reporting timelines.

**Cause:** DISA'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 collection 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'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's service organization in a timely manner, DISA 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 is unable to assert to the completeness and accuracy of reported FBWT on its Balance Sheet and other financial statement line items, as applicable.

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

1. Assist DISA's service organization by providing supporting information to clear transactions reported in SODs.
2. Continue working with Treasury, the Office of the Secretary of Defense (OSD), DISA's service organization, and other parties to transition away from using monthly NTDO reporting ALCs to daily TDO reporting ALCs.
3. Consider any limitations to DISA's service organization's SOD process and develop compensating controls to reconcile SOD balances to minimize the risk of a potential material misstatement.

4. Pursuant to receiving the necessary information and documentation from DISA's service organization, develop and implement procedures to identify DISA's actual or estimated SOD balances for recording and reporting adjustments within the financial statements.

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

1. Continue to develop procedures to determine what portion of the SOD balances, if any, should be attributed to DISA for financial reporting in a timely manner and made available for year-end financial reporting purposes.
2. Continue to monitor and track the resolution of SOD activity cleared to DISA 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. Continue to develop effective system and process controls to ensure that disbursements and collections are processed with valid TI, TAS, and FY inputs.
4. Assess and identify ALCs that primarily report collection and disbursement activity to Treasury on behalf of DISA.
5. Monitor and track the resolution of SODs cleared to DISA to enable DISA to perform root cause analysis and develop compensating controls for financial reporting purposes.
6. Coordinate recurring meetings with DISA to help resolve outstanding differences.

\* \* \* \* \*

## 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 2* presents the significant deficiencies identified during our audit.

***Exhibit 2: Significant Deficiencies and Sub-Categories***

Significant Deficiency	Significant Deficiency Sub-Categories
I. Property, Plant, and Equipment	A. Lack of Accountability over Property, Plant, and Equipment Assets B. Untimely Asset Activation
II. Budgetary Resources	A. Unfilled Customer Order Cutoff Issue
III. Financial Reporting	A. Agency Financial Report Omissions, Errors, and Noncompliance
IV. Information Technology	A. Defense Information Systems Agency Risk Management Framework B. Financial Accounting and Budget System Application Audit Logging and Monitoring C. Budget and Execution Reporting Tool Plan of Action and Milestones D. Financial Accounting Management Information System – Working Capital Fund Plan of Action and Milestones E. Incomplete Complementary User Entity Controls Implementation F. Incomplete Financial Accounting and Budget System Application Access Request Documentation G. Budget and Execution Reporting Tool Change Management Process

### I. Property, Plant, and Equipment (*Repeat Condition*)

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

- A. Lack of Accountability over PP&E Assets
- B. Untimely Asset Activation

#### A. Lack of Accountability over Property, Plant, and Equipment Assets

**Background:** The September 30, 2023 DISA WCF General Property, Plant, and Equipment (PP&E) was composed of leasehold improvements, equipment, software, assets under capital lease, and Construction-in-Progress (CIP) with a net book value (NBV) of \$1.01 billion.

During the inventory process, if PP&E assets are not located, a Property Custodian (PC) performs an informal inquiry to verify the assets are missing. When an asset is confirmed to be missing, the PC gathers all relevant information to complete a Financial Liability Investigation of Property Loss (FLIPL). The Capital Asset Management (CAM) Team then receives the FLIPL package, validates the FLIPL package for completeness, and searches records for the missing asset. If the asset is not located, the CAM Team updates its subledger system's (i.e., the Defense Property Accountability System [DPAS]) record status to "suspected loss." This results in an asset disposal from DISA's PP&E records. DISA management is responsible for developing policies and procedures to ensure that PP&E assets are accurately tracked and accounted for.

**Condition:** Testing for DISA's disposals found ineffective property accountability and inventory monitoring. Specifically, testing identified the following issues on a disposal sample size of 447 unique assets for an error rate of over 10% as of March 31, 2023 and a disposal sample size of 160 unique assets for an error rate of over 20% as of August 25, 2023:

- Fifty-four assets with an acquisition cost of \$6.0 million were unable to be located. DISA processed FLIPLs, and the assets were removed from DPAS
- Fourteen unique asset disposals with an acquisition cost of \$1.6 million were processed through FLIPL documentation and removed from DPAS, but then were later located. The assets were verified through re-establishment memos and will be added back to DPAS
- Eight unique asset disposals with an acquisition cost of \$583 thousand were processed through FLIPL documentation and removed from DPAS, but then were later located. The assets were verified through re-establishment memos; however, these assets were determined to no longer be needed in operation and will be disposed of
- Five unique equipment disposals with an acquisition cost of \$374 thousand were removed from DPAS. No FLIPLs were documented for these assets. The assets were subsequently found and will be added back to DPAS.

**Cause:** The majority of the asset disposals described above were uninstalled and sent to a warehouse by a DISA contractor. The PC did not track where the equipment was placed and was unable to locate and identify all the assets within the warehouse facility during inventory procedures. Additionally, assets were discovered to be incorrectly removed from DPAS while processing the FLIPL package and subsequently added back into DPAS.

**Effect:** DISA removed assets in the amount of \$8.6 million in acquisition cost from DPAS as of August 25, 2023, as the entity was unable to physically locate the assets. The lack of an effectively designed control increases the risk that misstatements will continue to occur and not be prevented, or detected and corrected, in a timely manner.

**Recommendations:** Kearney & Company, P.C. (Kearney) recommends that DISA perform the following:

1. Analyze the causes for its inability to locate assets during property inventories.

2. Consider control and process refinements to improve its property accountability. This may include additional accountability requirements for its contractors who could potentially un-install and/or relocate assets.

## **B. Untimely Asset Activation**

**Background:** The September 30, 2023 DISA WCF General PP&E was composed of leasehold improvements, equipment, software, assets under capital lease, and CIP with an NBV of \$1 billion. DISA utilizes DPAS as its property management system, which provides property financial reporting information.

Since fiscal year (FY) 2019, assets purchased using General Fund (GF) appropriations that will be utilized for the WCF are reported as CIP (United States Standard General Ledger [USSGL] Account 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's CAM Team receives e-mails from the site locations with the contract number and packing list, which DISA's CAM Team reviews to determine if the purchase includes capital assets.

In FY 2020, DISA implemented controls to identify equipment and labor costs received but not recorded in DPAS at FY-end. For direct shipments to DISA facilities, the receiving location notifies DISA's CAM Team via e-mail. DISA's 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 is responsible for establishing controls to record assets timely and accurately in DPAS.

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

- DISA did not record software with an NBV of \$5 million with a recorded activation date from FY 2022 in the correct FY and was unable to provide sufficient support for an FY 2023 activation date
- DISA did not transfer Equipment with an NBV of \$1 million in transfers from GF to the WCF in the correct FY
- DISA did not record \$21 thousand 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 officials who are responsible for property accounting. Additionally, DISA reported software purchases in FY 2023; however, the software was activated on September 30, 2022, consistent with the contract Period of Performance (PoP) and invoice date. DISA did not input the software into DPAS until FY 2023 and was unable to provide support showing that the software was not in use until FY 2023. Additionally, due to DISA's decentralized environment with equipment in

locations worldwide, DISA personnel do not always provide documentation to DISA's 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 \$6 million NBV on the PP&E line of the Balance Sheet and the General Equipment cost on Footnote 9 of the September 30, 2022 WCF financial statements. The untimely asset activation also resulted in an understatement of approximately \$430 thousand of depreciation on the Gross Costs line of the Statement of Net Cost (SNC) as of September 30, 2022. Therefore, this resulted in an overstatement of approximately \$430 thousand on the Gross Costs line of the SNC and an understatement of that amount on the Cumulative Results of Operations line of the Balance Sheet as of September 30, 2023. The lack of an effectively designed control increases the risk that a material misstatement could occur and not be prevented, or detected and corrected, in a timely manner.

**Recommendations:** Kearney recommends that DISA perform the following:

1. Further develop an effective control and process to monitor assets for timely activation and ensure they are recorded in the financial statements in a timely manner via JV if received after the DPAS downtime 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 PCs on asset shipments.
4. Conduct annual PP&E inventory to ensure assets noted on the inventory are identified in the current FY's financial statements.
5. Increase communication between DISA's CAM Team, DISA's Financial Management Team, and 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.
6. Develop and implement a process to ensure and document that software is activated and recorded in the correct FY.

## **II. Budgetary Resources (*New Condition*)**

### **A. Unfilled Customer Order Cutoff Issue**

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

The DISA WCF reported approximately \$871.6 million in UCOs Without Advance on its September 30, 2023 trial balance. The account balance is supported by a subsidiary ledger that details information such as the fund, document number, order amount, and transaction date, among other unique identifying details for each UCO balance.

DISA is responsible for developing policies and procedures to ensure that customer orders are accurately reported in the correct FY.

**Condition:** DISA WCF entered into finalized MIPRs during FY 2023 for \$61.9 million; however, the corresponding UCOs were not recorded until FY 2024. Within the results, \$52.26 million was identified through FY cutoff procedures, and DISA WCF management performed an analysis which identified an additional \$9.65 million.

**Cause:** DISA management elected to delay recording UCOs accepted at the end of FY 2023 until FY 2024, as the obligations to fulfill the customer orders would not be awarded until FY 2024. However, Federal accounting guidance requires that the order be recorded once the agreement was accepted, regardless of whether the order was for obligations to be executed in the next FY. DISA management delayed the recording of the UCOs to avoid inflating their budget authority received in FY 2023, even though the UCO was signed in FY 2023. DISA management did not have internal control procedures to ensure that the UCOs were recorded in the correct FY.

**Effect:** The DISA WCF Statement of Budgetary Resources (SBR) Line 1890, *Spending Authority from Offsetting Collections (discretionary and mandatory)*, was understated by \$61.9 million as of September 30, 2023. Additionally, DISA completed an analysis of the remaining UCOs recorded in FY 2024 and determined that most likely no additional cutoff issues existed beyond what is noted in the finding.

**Recommendation:** Kearney recommends that DISA perform the following:

1. Develop and document procedures to ensure that UCOs are recorded in the FY in which the customer order is established.

### **III. Financial Reporting (*Repeat Condition*)**

#### **A. Agency Financial Report Omissions, Errors, and Noncompliance**

**Background:** DISA utilizes a service organization for financial reporting assistance. The service organization performs financial statement compilation and reporting within the Defense Departmental Reporting System (DDRS) – Budgetary (B) and DDRS – Audited Financial Statements (AFS). DISA management is responsible for the compilation of financial information into DISA’s Agency Financial Report (AFR), as well as the accuracy, completeness, and presentation and disclosure of the information reported within. DISA is also responsible for ensuring that the AFR is prepared and presented in compliance with Office of Management and



Budget (OMB) Circular A-136, *Financial Reporting Requirements*. Each quarter, including at FY-end, DISA management completes and signs a checklist of items and tasks to complete as it prepares its financial statements and financial statement notes and disclosures. DISA utilizes multiple resources in receiving feedback to incorporate changes throughout the FY (e.g., Office of the Under Secretary of Defense [Comptroller] [OUSDC], its service organization, independent audit firms) within the AFR. Additionally, DISA is responsible for ensuring all quality control (QC) reviews occur and compliance updates are made prior to publication.

**Condition:** The DISA WCF Quarter (Q) 4 draft AFR contained omissions, errors, and instances of noncompliance not identified by DISA management. There were minor rounding errors when comparing information reported in multiple places throughout the AFR (e.g., differences between an amount presented in a footnote vs. the same information in the relevant financial statement). The AFR also contained numerous editorial errors that were not detected and corrected throughout the QC review process. In addition, there were various missing and omitted OMB Circular A-136 components that were noted during reviews of the draft AFR, such as the following:

- **Section II.1.1:** Missing statement providing reasonable assurance over the completeness and reliability of the financial data used in the reports and in describing material weaknesses and the actions the agency is taking to resolve them
- **Section II.2.2:** Inconsistent major programs described in Management's Discussion and Analysis (MD&A) compared to the SNC
- **Section II.3.8.33:** Omitted the required disclosure on DISA WCF's related party activity.

**Cause:** Although it has implemented various remediation efforts and coordinated multiple draft AFR submissions for review prior to the noted deadlines, DISA does not yet have the necessary control environment and consistent QC processes to ensure the content of the AFR is complete, accurate, and in compliance with OMB Circular A-136 requirements. Prior to its final AFR submission to the specific requesting parties (e.g., independent audit firms, OUSDC), DISA relies on its service organization to prepare its AFR. The division of responsibilities between DISA and the service organization for ensuring the effectiveness of that review has not yet been sufficiently delineated, as demonstrated by the discrepancies and errors identified and communicated to DISA during the audit. **Effect:** DISA made various corrections and incorporated updates to the additional information included in its FY 2023 AFR prior to finalization in order to ensure the document complied with the appropriate OMB requirements. However, without appropriate controls and QC processes, there is an increased risk that DISA's AFR will not be complete, accurate, and compliant with OMB requirements in future periods.

**Recommendations:** Kearney recommends that DISA perform the following:

1. Continue to review, implement, and document the processes and internal control environment relating to the accumulation and review of the data utilized to prepare the AFR and confirm that disclosures, supporting tables, reconciliations, and analytical information reported in the AFR are reasonable and accurate.
2. Continue to create, develop, and document additional procedures and/or checklists to:

- a. Identify all relationships of information within the AFR to ensure consistency in the content presented.
- b. Ensure all the information compiled into the AFR is reviewed at a sufficient level by DISA management to ensure accuracy, completeness, and compliance with requirements.
- c. Document evidence of the detail review(s).

#### **IV. Information Technology (*Repeat Condition*)**

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

- A. Defense Information Systems Agency Risk Management Framework
- B. Financial Accounting and Budget System Application Audit Logging and Monitoring
- C. Budget and Execution Reporting Tool Plan of Action and Milestones
- D. Financial Accounting Management Information System – Working Capital Fund Plan of Action and Milestones
- E. Incomplete Complementary User Entity Controls Implementation
- F. Incomplete Financial Accounting and Budget System Application Access Request Documentation
- G. Budget and Execution Reporting Tool Change Management Process

##### **A. Defense Information Systems Agency Risk Management Framework**

**Background:** As a U.S. Department of Defense (DoD) Combat Support Agency, DISA provides enterprise services, unified capabilities, and mobility options to support DoD worldwide operations. DISA meets the DoD’s information technology (IT) needs through enterprise security architectures, smart computing options, and other leading-edge IT opportunities. Specifically, DISA delivers hundreds of IT support services 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 and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle. Executing the RMF tasks links essential risk management processes at the system level to risk management processes at the



organization level. In addition, it establishes responsibility and accountability for the controls implemented within an organization's information systems and inherited by those systems.

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

The CNSS collaborates with NIST to ensure NIST SP 800-37 (as amended), NIST SP 800-53, and NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, address security and privacy safeguards to meet the requirements of NSSs to the extent possible and provide a common foundation for information security and privacy across the U.S. Federal Government.

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 OMB Circular A-130, *Managing Information as a Strategic Resource*, organizations have a one-year grace period prior to finalizing their implementation of any updated requirements.

**Condition:** DISA did not update its RMF documentation, processes, or procedures to reflect updated requirements presented within NIST SP 800-53, Rev. 5 and NIST SP 800-53A, Rev. 5 in the prescribed timeline set forth by OMB Circular A-130, Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources" (i.e., one-year implementation post-publication). Furthermore, DISA personnel did not revise their system-specific security documents, such as System Security Plans (SSP), or related documentation (e.g., Security Design Documents [SDD]) to reflect requirements detailed in NIST SP 800-53, Rev. 5.

**Cause:** The DoD Chief Information Officer (CIO) began the process of formally adopting NIST SP 800-53, Rev. 5 following the adoption of CNSSI No. 1253, Rev. 5 in July 2022. Full adoption of NIST SP 800-53, Rev. 5 will include an update to DoD policies, baselines, eMASS, and the Security Controls Explorer on the RMF Knowledge Service (KS). The DoD is developing guidance for the transition to NIST SP 800-53, Rev. 5 with system transition timelines estimated to range from within six months of DoD Rev. 5 adoption to three years depending on a system's authorization status. This includes updating DoD-Specific Assignment Values for security controls, as well as assessment procedures. As of April 2023, the DoD completed updates to the CNSSI No. 1253 baselines and pre-loaded eMASS with the updated controls from NIST SP 800-53, Rev. 5.

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

**Recommendations:** Kearney recommends that DISA perform the following:

1. Continue to monitor the DoD's ongoing efforts to formally adopt NIST SP 800-53, Rev. 5 and remain up to date regarding updates to relevant control baselines, overlays, and eMASS.
2. Once the DoD transition plan is released, develop and implement plans to transition DISA's RMF and systems and update system-specific assessment and security documentation, including control selection and implementation, to reflect requirements detailed in NIST SP 800-53, Rev. 5 within the required timeframe.

## **B. Financial Accounting and Budget System Application Audit Logging and Monitoring**

**Background:** Financial Accounting and Budget System (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 (TSEAS) Defense Working Capital Fund (DWCF). Financial transactions are sent from the Contracting Online Procurement System (COPS) to FABS, which generate Accounts Payable (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 (USF).

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, as well as for providing information useful for resolving such problems. Logs can also be helpful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems. In addition, organizations should establish policies and procedures for log management, prioritize log management appropriately, and provide proper support for all staff with log management responsibilities.

DISA utilizes a Virtual Storage Access Method (VSAM) Cluster File, which is a system library that cannot be changed by Database Administrators (DBA) to run the audit logs report for the FABS application. DISA personnel run the VSAM Cluster File containing four types of files (i.e., C\$US, C\$SP, C\$AP, C\$MN) monthly.

**Condition:** DISA developed a process to log security authorization modifications (i.e., modifications to existing users' account privileges) for the FABS application; however, the

process did not incorporate timely review, nor documentation detailing how personnel would complete the review. For example, DISA did not finalize documentation detailing a process to perform a review, including the frequency of review, maintenance of review documentation, and documentation of actions taken as a result of the review. Furthermore, DISA did not adhere to the required frequency (i.e., seven days) for audit logs review.

**Cause:** As of April 2023, DISA personnel had developed and improved their process to log all security authorization modifications to the FABS application to include performing review over the generated audit logs. However, due to timing constraints, DISA was unable to finalize documentation surrounding the process in DISA-specific policies and procedures for the FABS application to include actions taken on account modifications captured.

**Effect:** By not reviewing and documenting the actions taken on the audit logs for the FABS application in a consistent and timely manner, DISA personnel may not be aware of potential issues that could affect the integrity and availability of the FABS application. In addition, untimely audit log reviews may result in inappropriate or malicious actions remaining undetected for an extended period, which may hinder DISA's ability to initiate prompt corrective action.

**Recommendations:** Kearney recommends that DISA perform the following:

1. Finalize documented procedures to regularly review and document FABS security authorization modifications at the application layer. This documentation, at a minimum, should identify which events are logged, which events require manual review and why, who performs the review, the frequency of the review, how the individuals responsible for the review remain independent from reviewing their own work, how the logs are protected from inappropriate tampering, and which events require escalation.
2. Ensure review of the FABS application logs are completed within prescribed timelines (i.e., seven days), as required by DoD-wide guidance, and retain evidence of the review of FABS application logs for third-party review.
3. Update applicable FABS policy and procedural documentation to reflect the newly developed application audit log and review process.
4. Develop and implement a QC process over the FABS application logging and monitoring review process. The QC process should include procedures to ensure FABS application logs are reviewed within the prescribed timeline and that personnel are not the sole reviewer over processes for which they are responsible on a day-to-day basis.

### **C. Budget and Execution Reporting Tool Plan of Action and Milestones**

**Background:** Budget and Execution and Reporting Tool (BERT) provides the cost center manager with a standard method of creating budget packages which are forwarded to Headquarters. The system also provides a means for tracking the actual execution of the approved budget. BERT is a dynamic system which provides the capability to update labor workload, budget, and payroll projections. The execution of the budget projections can be compared to an approved budget. A process for the development of billing rates is provided. The Chargeback application is used to process and validate charges (utilization) and billing data.



The Project Management application can be used to monitor estimates, funding, and the execution of client-supported projects.

NIST SP 800-37, Rev. 2 informs individuals associated with the design, development, implementation, operation, maintenance, and disposition of Federal information systems about how to conduct risk assessments, security categorizations, security control selections and implementations, security control assessments, information system authorizations, and monitoring of security controls.

Further, NIST SP 800-37, Rev. 2 requires that a designated authorizing official (AO) authorize agency information systems to operate. As part of the authorization process, the agency must develop, track, and manage a comprehensive Plan of Action and Milestones (POA&M) for known system weaknesses. OMB Memorandum (M)-02-01, *Guidance for Preparing and Submitting Security POA&Ms*, provides specific POA&M guidance to agencies, including guidance on sources of security weaknesses. DISA utilizes eMASS to develop, track, and manage POA&Ms. However, DISA Accounting Integration Branch (CFA33) is not responsible for any inherited controls (i.e., physical security controls handled by the DISA Datacenters). If the Information System Security Manager (ISSM) assesses a control categorized as compliant in eMASS to be noncompliant, he/she must generate a related POA&M in eMASS, and the group owning the control environment is responsible for the POA&Ms related to noncompliant inherited controls. Due to systematic limitations within eMASS, DISA is unable to create POA&Ms for inherited controls categorized as compliant. To remediate its inability to create POA&Ms for inherited controls, DISA chose to document findings as artifacts retained in eMASS and provided to the AO as part of the authorization package prior to authorization.

**Condition:** DISA's POA&M management process did not capture all security weaknesses found within BERT during reviews done by, for, or on behalf of the agency as required by OMB M-02-01. Specifically, DISA did not develop, track, and manage POA&Ms for security weaknesses found within BERT Notices of Findings and Recommendations (NFR) (i.e., NFRs 2022-IT-WCF-03, *Inconsistent BERT Change Management Process*, and 2022-IT-WCF-07, *BERT Database Audit Logging and Monitoring*) issued during the FY 2022 financial statement audit.

**Cause:** As of April 2023, DISA had not been tracking system-level POA&Ms in eMASS in relation to the BERT application. DISA uploaded the related Corrective Action Plan (CAP) for the prior-year BERT NFRs into eMASS on April 17, 2023, after the reauthorization of the BERT application on January 13, 2023. As such, the BERT AO granted the BERT application authorization without formal POA&M entries or CAPs to track prior-year application-specific findings, known weaknesses, and/or deficiencies related to the BERT application. While DISA management stated that CAPs and POA&Ms contain the same information and, therefore, did not deem it necessary to develop POA&Ms to track and manage NFRs related to BERT security weaknesses identified during the FY 2022 financial statement audit, DISA management did not upload the CAP documentation into eMASS prior to the BERT application authorization process.

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

**Recommendations:** Kearney recommends that DISA perform the following:

1. Enhance its formal POA&M management process to ensure personnel develop, track, and manage POA&Ms for all applicable security weaknesses per OMB M-02-01, including those found during reviews done by, for, or on behalf of the agency (i.e., NFRs issued during financial statement audits).
2. Supplement its POA&M Tactics, Techniques, and Procedures (TTP) with the *DISA Cybersecurity Policy* or equivalent Standard Operating Procedures (SOP) to ensure a repeatable POA&M management process with consistent communication of security weaknesses from all required sources.
3. Maintain findings, POA&Ms, or artifacts within eMASS to ensure that the AO is aware of all security weaknesses identified when making an authorization decision.

#### **D. Financial Accounting Management Information System – Working Capital Fund Plan of Action and Milestones**

**Background:** The Financial Accounting Management Information System (FAMIS) – WCF is the core financial accounting system for the DWCF Business Area. FAMIS-WCF addresses Federal, DoD, and DWCF requirements by: 1) recording financial transactions from both direct entry and via automated batch interfaces with both internal and external critical feeder systems; 2) providing the ability to inquire on a specific item (e.g., receivable document, customer account, payable document, vendor account, GL account, or directorate budget); and 3) producing monthly financial statements in a variety of formats for internal and external distribution. The FAMIS-WCF system is an upgrade of the FAMIS legacy system using Oracle E-Business (R12) platform.

NIST SP 800-37, Rev. 2 informs individuals associated with the design, development, implementation, operation, maintenance, and disposition of Federal information systems about how to conduct risk assessments, security categorizations, security control selections and implementations, security control assessments, information system authorizations, and monitoring of security controls.

Further, NIST SP 800-37, Rev. 2 requires that a designated AO authorize agency information systems to operate. As part of the authorization process, the agency must develop, track, and manage a comprehensive POA&M for known system weaknesses. OMB M-02-01 provides specific POA&M guidance to agencies, including guidance on sources of security weaknesses. DISA utilizes eMASS to develop, track, and manage POA&Ms. However, DISA CFA33 is not responsible for any inherited controls (i.e., physical security controls handled by the DISA Datacenters). If the ISSM assesses a control categorized as compliant in eMASS to be

noncompliant, he/she must generate a related POA&M in eMASS, and the group owning the control environment is responsible for the POA&Ms related to noncompliant inherited controls. Due to systematic limitations within eMASS, DISA is unable to create POA&Ms for inherited controls categorized as compliant and as a solution to the inability to create POA&Ms for inherited controls, DISA chose to document findings as artifacts retained in eMASS and provided to the AO as part of the authorization package prior to authorization.

**Condition:** DISA's POA&M management process did not capture all security weaknesses found within FAMIS-WCF during reviews done by, for, or on behalf of the agency as required by OMB M-02-01. Specifically, DISA did not develop, track, and manage POA&Ms for security weaknesses found within FAMIS-WCF NFRs (NFR #2022-IT-WCF-06, *FAMIS-WCF Removal of Inactive and Separated Users*, and NFR #2022-IT-WCF-08, *FAMIS-WCF Database Audit Logging and Monitoring*) issued during the FY 2022 financial statement audit.

**Cause:** As of April 2023, DISA had not been tracking system-level POA&Ms in eMASS in relation to the FAMIS-WCF application. DISA uploaded the related CAP for the prior-year FAMIS-WCF NFRs into eMASS on April 17, 2023 after the reauthorization of the FAMIS-WCF application on January 13, 2023. As such, the FAMIS-WCF AO granted the FAMIS-WCF application authorization without formal POA&M entries or CAPs to track prior-year application-specific findings, known weaknesses, and/or deficiencies related to the FAMIS-WCF application. While DISA management stated that CAPs and POA&Ms contain the same information and, therefore, did not deem it necessary to develop POA&Ms to track and manage NFRs related to FAMIS-WCF security weaknesses identified during the FY 2022 financial statement audit, DISA management did not upload the CAP documentation into eMASS prior to the FAMIS-WCF application authorization process.

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

**Recommendations:** Kearney recommends that DISA perform the following:

1. Enhance its formal POA&M management process to ensure personnel develop, track, and manage POA&Ms for all applicable security weaknesses per OMB M-02-01, including those found during reviews done by, for, or on behalf of the agency (i.e., NFRs issued during financial statement audits).
2. Supplement its POA&M TTP with the DISA Cybersecurity Policy or SOP to ensure a repeatable POA&M management process with consistent communication of security weaknesses from all required sources.
3. Maintain findings, POA&Ms, or artifacts within eMASS to ensure the AO is aware of all security weaknesses identified when making an authorization decision.



## **E. Incomplete Complementary User Entity Controls Implementation**

**Background:** DISA utilizes several service organizations to support its operations and mission. As such, DISA obtains assurances from each organization regarding the effectiveness of the organization's internal controls related to the service(s) provided. Specifically, each organization provides a written assertion that accompanies a description of its service(s) and related information system(s). These assertions are communicated via a System and Organization Controls (SOC) report. In FY 2023, 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., clients or users of the service[s]) will implement certain controls (i.e., complementary user entity controls [CUEC]) to achieve the overall control objectives and create a secure computing environment. Specifically, Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification*, defines CUECs as “controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the service organization's system.”

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

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

- DISA did not develop cross-system SD documentation to detail conflicts that may occur when personnel obtain access to multiple systems utilized by DISA to include, but not be limited to, ADS, Advana, DAI, DCAS, DCPS, DCPDS, DDRS, DPAS, and WAWF

- DISA did not effectively perform periodic reviews of all DISA users for the Advana application
- DISA did not maintain adequate documentation to support management's approval of the level of access granted to DISA users of the DAI and DCPS applications
- DISA did not consistently remove or disable access to DISA users of the DAI and WAWF applications upon their separation from the agency.

**Cause:** Although DISA was aware of the requirements for implementing the CUECs and had begun implementation, it had not finalized implementation of all CUECs as of the end of the FY 2023 financial statement audit. Throughout FY 2023, DISA refined its existing process regarding review and implementation of all CUECs identified within each service organization's SOC 1®, Type 2 report, determined relevance to DISA and assessed its corresponding DISA control, as well as continued to identify and implement controls to remediate gaps for CUECs not sufficiently designed (e.g., cross system SD). Additionally, due to the large number of CUECs, DISA established a phased approach and executed it to test CUECs based on level of risk and document results of implementation.

**Effect:** DISA'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.

**Recommendations:** Kearney recommends that DISA 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 effectively; design and implement controls to remediate those gaps.

#### **F. Incomplete Financial Accounting and Budget System Application Access Request Documentation**

**Background:** 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 TSEAS DWCF. Financial transactions are sent from COPS 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 USF.

DISA 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 request access. 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 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 by the FABS Data Owner (DO) for processing. The SA group identifies the applicable DO residing in DISA's Office of Accounting Operations and Compliance (CFA) or Defense Information Technology Contracting Organization (DITCO) – 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 information systems 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 was unable to provide sufficient documentation to support that management reviewed and approved the access permissions granted for five out of 12 users (~42%) who received access to the FABS application from October 1, 2022 through April 24, 2023. Specifically, DISA did not validate requested access, granted access to incorrect facility codes, and was unable to provide evidence of requested facility codes (e.g., permissions).

**Cause:** DISA personnel updated the user authorization process for FABS for access request through ESPS/SAM. These updates included an automatic SAAR form built into ESPS/SAM that users utilize to request access. However, though the SAAR forms incorporated a section for facility code selection, some users did not select a facility code but, instead, requested for their access to match that of another user, while other users requested access using the wrong access request form (i.e., no section for facility code selection). Additionally, as part of the access authorization process, DISA did not have an effective QC process to ensure system administrators review user access request forms properly, thereby resulting in incorrect access being granted to users.

**Effect:** By failing to ensure a facility code selection or validate requested roles before granting access to the FABS application, there is increased risk that users may obtain inappropriate access to the FABS application.

**Recommendations:** Kearney recommends that DISA perform the following:

1. Develop and implement a QC review over the user authorization process. The QC process should include procedures to ensure completion of the access request form in ESPS/SAM for all FABS users (internal and external) and validating requested roles. To gain efficiencies, DISA should consider incorporating this QC process as it conducts its audit log reviews of account creations and modifications.
2. Update the user authorization process to include selection of a facility within the access request form in ESPS/SAM.

## **G. Budget and Execution Reporting Tool Change Management Process**

**Background:** BERT provides the cost center manager with a standard method of creating budget packages which are forwarded to Headquarters. The system also provides a means for tracking the actual execution of the approved budget. BERT is a dynamic system which provides the capability to update labor workload, budget, and payroll projections. The execution of the budget projections can be compared to an approved budget. A process for the development of billing rates is provided. The Chargeback application is used to process and validate charges (utilization) and billing data. The Project Management application can be used to monitor estimates, funding, and the execution of client-supported projects.

DISA utilizes SharePoint Online to manage the BERT application change management (CM) process from initiation through implementation via change “states” (i.e., Submitted, Approved, Analysis, Development, Testing, Review, Implementation, Verification, and Closed). The CM process begins when an individual with access to SharePoint Online submits a Change Request (CR). The CR must undergo a Change Control Board (CCB) approval process and flow through development and/or test environments before migrating to the BERT production environment. If a CR fails testing, SharePoint Online will route the change back to the Developer, and the development and testing processes may undergo several iterations to ensure the change does not affect the stability of the BERT production system upon implementation. Once the Tester approves the CR in the development environment, SharePoint Online routes the CR to the CCB Chairperson for a final management review and approval. Once the CCB Chairperson approves the CR, SharePoint Online notifies the technical point of contact (POC) that the approved changes are ready for migration to the BERT production environment. Once the change is implemented into the BERT production environment, SharePoint Online requires that the appropriate personnel log a post-implementation verification prior to closing the CR.

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

Additionally, per NIST SP 800-128, a CCB or equivalent group is identified for the review and approval of configuration changes for the system. The CCB plays a key role as gatekeeper in deciding which changes may be acted upon and introduced into a system. The CCB deliberately considers the potential effect of a proposed change on the functionality and secure state of the system and risk to the mission, should the change be implemented in the context of the risk tolerance established by the organization. By reviewing each proposed and implemented

modification, the CCB ensures that there is a disciplined, systematic, and secure approach for introducing change.

**Condition:** DISA personnel did not ensure all BERT application changes followed a defined and controlled process in accordance with DISA’s policies and procedures. Specifically, DISA did not document testing and approval for one out of 21 changes (~5%) implemented into production in FY 2023.

**Cause:** In FY 2023, DISA personnel improved the BERT application CM processes and procedures. These improvements included updates to BERT CM procedural documentation to reflect current roles and responsibilities of the BERT CCB and references to the CM repository implemented in FY 2022. Further, DISA personnel maintained a complete and accurate listing of changes implemented into the BERT production environment.

However, DISA personnel did not provide adequate training to new BERT Developers to ensure Developers were up to date with the documented BERT CM processes. Specifically, DISA personnel stated that a new Developer was not proficient in updating the BERT tracker application (CFA33 Pensacola Change Request Tracker) with required CR state changes (i.e., Submitted, Approved, Analysis, Development, Testing, Review, Implementation, Verification, and Closed). However, upon identification of the missing documentation requirements, DISA personnel provided training to the BERT Developer regarding the proper BERT CM workflow/processes. Additionally, DISA personnel provided documentation to support identification of lack of approvals and the remediation efforts taken (i.e., creating and providing training) to ensure the lack of thorough documentation did not occur in the future.

**Effect:** By failing to maintain sufficient documentation to support all required phases of the CM process, DISA personnel may not be fully aware of changes implemented into the BERT production. In addition, implementing changes prior to obtaining approval and adequate testing increases the risk that vulnerabilities may be introduced into the BERT production environment which could impact the security posture of the information system and organization.

**Recommendations:** Kearney recommends that DISA perform the following:

1. Consistently follow the updated BERT CM processes to ensure approval and testing of changes are documented and effectively tracked in the CFA33 Change Request Tracker within SharePoint Online prior to implementation into the production environment.
2. Consistently update the CFA33 Change Request Tracker with detailed information regarding state changes from initial CR through the implementation stage.
3. Improve and implement the QC review procedures to supplement the BERT configuration CM process. The QC reviews should ensure that all BERT changes follow a defined and controlled process, including maintaining appropriate supporting documentation for all CRs implemented into the production environment.



## APPENDIX A: STATUS OF PRIOR-YEAR DEFICIENCIES

In the *Independent Auditor's Report on Internal Control over Financial Reporting* included in the audit report on the Defense Information Systems Agency (DISA) Working Capital Fund's (WCF) fiscal year (FY) 2022 financial statements, we noted several issues that were related to internal control over financial reporting. The statuses of the FY 2022 internal control findings are summarized in *Exhibit 3*.

*Exhibit 3: Status of Prior-Year Findings*

<b>Control Deficiency</b>	<b>FY 2022 Status</b>	<b>FY 2023 Status</b>
<b>Fund Balance with Treasury</b>	Material Weakness	Material Weakness
<b>Property, Plant, and Equipment</b>	Material Weakness	Significant Deficiency
<b>Budgetary Resources</b>	Not Applicable (N/A)	Significant Deficiency
<b>Financial Reporting</b>	Significant Deficiency	Significant Deficiency
<b>Information Technology</b>	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. 24-01, *Audit Requirements for Federal Financial Statements*, the Working Capital Fund (WCF) financial statements of the Defense Information Systems Agency (DISA) as of and for the year ended September 30, 2023 and the related notes to the financial statements, which collectively comprise DISA WCF's financial statements, and we have issued our report thereon dated December 15, 2023.

**Report on Compliance and Other Matters**

As part of obtaining reasonable assurance about whether DISA WCF's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of the financial statement amounts, and provisions referred to in Section 803(a) of the Federal Financial Management Improvement Act of 1996 (FFMIA). We limited our tests of compliance to these provisions and did not test compliance with all laws, regulations, contracts, and grant agreements applicable to DISA WCF. However, providing an opinion on compliance with those provisions was not an objective of our audit; accordingly, we do not express such an opinion. The results of our tests, exclusive of those referred to in FFMIA, disclosed an instance of noncompliance or other matter that is required to be reported under *Government Auditing Standards* and OMB Bulletin No. 24-01 and which is described in the accompanying **Schedule of Findings** as Item I.

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

**DISA 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 (AFR). DISA WCF concurred with the findings identified in our



engagement. DISA WCF's response was not subjected to the other auditing procedures applied in the audit of the financial statements; accordingly, we express no opinion on the response.





### **Purpose of this Report**

The purpose of this report is solely to describe the scope of our testing of compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 24-01 in considering the entity's compliance. Accordingly, this report is not suitable for any other purpose.

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

Alexandria, Virginia  
December 15, 2023

## Schedule of Findings

### Noncompliance and Other Matters

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

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

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

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

- Material Weakness:
  - Fund Balance with Treasury (FBWT)
- Significant Deficiencies:
  - Property, Plant, and Equipment (PP&E)
  - Budgetary Resources
  - Financial Reporting
  - Information Technology (IT).

## **DISA Management Comments to Auditor's Report**



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

Mr. Gorrell:

DISA acknowledges receipt of Kearney & Company's audit report for DISA's FY 2023 Working Capital Fund (WCF) financial statements.

We acknowledge the auditor-identified findings in the following key area:  
1) Fund Balance with Treasury which in the aggregate is considered a material weakness. We also acknowledge the auditor-identified findings in the following key areas: 1) Property, Plant and Equipment, 2) Budgetary Resources, 3) Financial Reporting, and 4) Information Technology each of which, in the aggregate are considered significant deficiencies.

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

SPONSELLER.JU  
STIN.C.1258339  
246

Digitally signed by  
SPONSELLER.JUSTIN.C.1258339  
Date: 2023.12.13 09:36:46  
-05'00'

For, ALEX DIAZ  
Director, Accounting Operations  
and Compliance

## **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