Defense Information Systems Agency
Working Capital Fund
Agency Financial Report
Fiscal Year 2025

About the Defense Information Systems Agency Financial Report

This Fiscal Year (FY) 2025 Agency Financial Report (AFR) refers to the Department of Defense (DoD) in accordance with statutory requirements. While mindful of the recent *Executive Order 14347* and ongoing legal determinations regarding the Department's name, this report utilizes the designation "Department of Defense" because the AFR is a statutorily mandated report, all relevant legislation designates the Department as the "Department of Defense," and the funding for programs discussed herein were issued to the Department of Defense. We may use the "Department of War" designation in other, non-statutory communications, as allowed by the Executive Order.

Message From the Defense Information Systems Agency

As the Defense Information Systems Agency (DISA) director, I am pleased to present the Agency Financial Report (AFR) for the DISA Working Capital Fund (WCF), as of Sept. 30, 2025. The information presented in this AFR, along with its accompanying footnotes, encompasses the required management discussion and analysis, performance data, and financial statements. The AFR has been prepared according to the guidelines outlined in Office of Management and Budget Circular A-136 and includes the auditor's signed report. As agency head, I have evaluated the financial and performance data within this report and am confident in its completeness and reliability. Further details regarding this assessment and its resulting actions are provided in this letter.

In FY 2025, DISA continues to be a trusted partner throughout the Department of Defense (DoD), leading the way in providing information technology (IT) and telecommunication support to our warfighters. We safeguard communications to enable our nation's success, from the battlefield to the White House. We deploy, maintain and secure a comprehensive suite of command, control and communications capabilities, along with a universally accessible information infrastructure. This enables our military to maintain a lethal advantage, fight when necessary and win – on land, at sea, in the air, space and in cyberspace. DISA's strategy for FY 2025-2029, DISA Next, outlines how the agency is solving enterprise-level, hard, and complex IT and telecommunications problems. DISA's priorities center around first, **Readiness** emphasizes ensuring personnel are well-trained, confident, and prepared to execute as a cohesive team. Second, **Campaigning** focuses on understanding the mission and effectively leveraging resources to deliver impactful solutions to the Warfighter. Third, **Continuous Modernization** encourages embracing innovation and strategically shaping the cyber terrain to our advantage. Finally, **Establish Lethality** requires developing and deploying superior capabilities to maintain an advantage over evolving threats.

Based on feedback from Kearney & Company, our independent public accounting (IPA) firm, we continue to improve financial processes. Beginning in FY 2024, and in FY 2025, the DISA WCF sustains no material weaknesses. The IPA has reported significant control deficiencies, which DISA is addressing through mitigating controls, specifically in Fund Balance with Treasury; cash management report creation; suspense account and statement of differences reconciliation and reporting processes; and property plant, and equipment. Corrective action plans are in place to address identified deficiencies in DISA's WCF financial statements. We are expanding our use of robotic process automation to gain further efficiencies. These improvements contribute to a sound internal control environment, enabling DISA to effectively execute its strategy, prioritize readiness through innovation, and improve cost management. The DISA WCF continues enhancements through updated internal controls, such as Identity, Credential, and Access Management (ICAM), and to improve accuracy, efficiency, and decision-making. DISA can provide reasonable assurance of the effective operation of internal controls over financial reporting, operations, and compliance as of Sept. 30, 2025, and has achieved this success since FY 2019.

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

Table of Contents

DISA Working Capital Fund

Management's Discussion and Analysis

Fiscal Year 2025, Ending Sept. 30, 2025

The Defense Information Systems Agency (DISA) is pleased to present a Management's Discussion and Analysis (MD&A) to accompany its fiscal year (FY) 2025 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**

Context for the Financial Information in the MD&A

History and Enabling Legislation

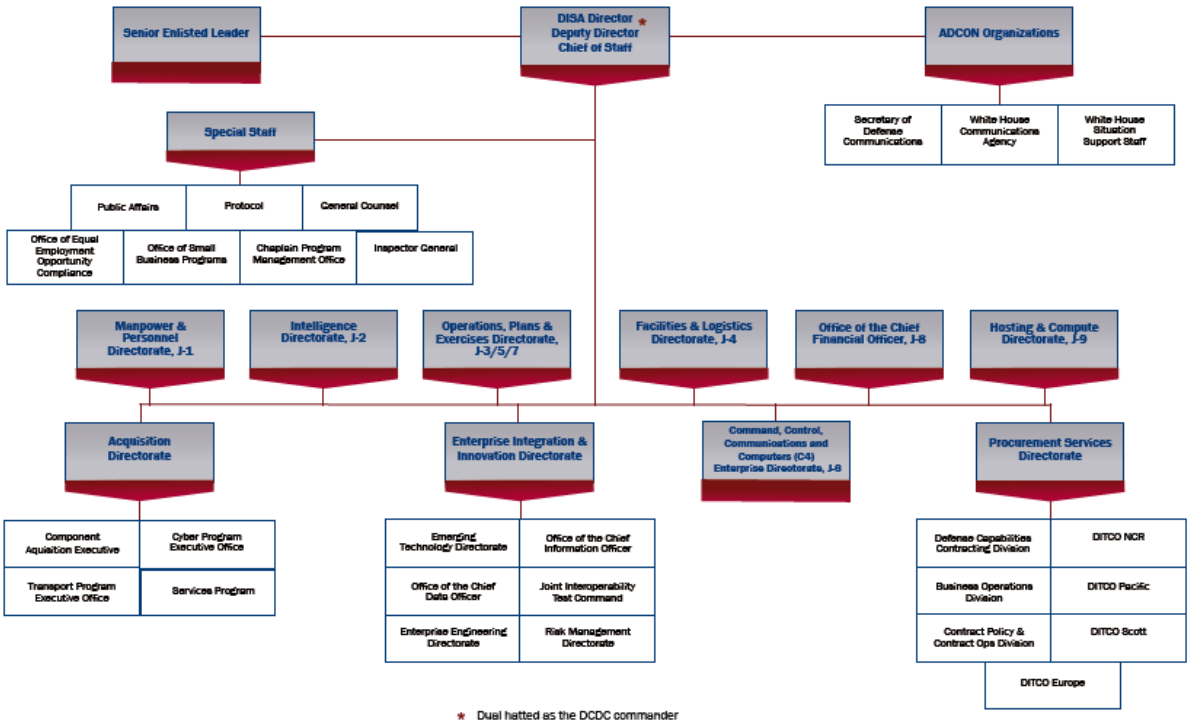
DISA, a combat support agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support of joint warfighters, national level leaders, and other mission and coalition partners across the full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

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

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

Organization

To fulfill its mission and meet strategic plan objectives, DISA operates under the direction of the DoD CIO, who reports directly to the secretary of defense. The organizational structure for DISA as of September 2025 is depicted below:



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

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

DISA's Defense Working Capital Fund (DWCF)

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

A DWCF business unit is not profit-oriented and therefore only tries to break even, charging prices set using the full-cost-recovery principle, which accounts for all costs — both direct and indirect (or

"overhead") costs. It is intended to generate adequate revenue to cover the full cost of its operations and to finance the fund's continuing operations without fiscal year limitation.

DISA operates the information services activity within the DWCF. This activity consists of three main programs that make up the One Fund: Telecommunications Services (TS) Program Element (PE) 55, Enterprise Acquisition Services (EAS) (PE56) and Computing Services (CS) (PE54). These are the programs that make up the Statement of Net Cost.

The major element of the TS (PE55) component is the Defense Information Systems Network (DISN), which provides interoperable telecommunications connectivity and accompanying services that allow the department to plan and operate both day-to-day business and operational missions through the dynamic routing of voice, data, text, still and full-motion imagery, and bandwidth services. Some DISN services are provided to mission partners in predefined packages and sold on a subscription basis via the DISN subscription service, while others are made available on a cost- reimbursable basis.

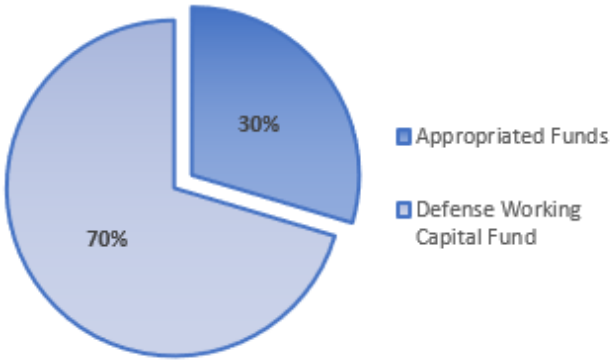
The EAS (PE56) enables the department to procure the best value, commercially competitive IT services and capabilities through DISA's Defense IT Contracting Organization (DITCO). DITCO provides complete contracting support and services.

The CS (PE54) component of DISA's DWCF activities operates DISA data centers, which provide mainframe and server-processing operations, data storage, production support, technical services, and end-user assistance for command and control, combat support, and enterprise applications across DoD. These facilities and functions provide a robust enterprise computing environment to more than 4 million users through 17 mainframes; approximately 10,000 servers; 73 petabytes of storage data; 3,400 network devices and 235,000 square feet of raised floor.

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

BUDGET

Appropriated	$3.7 Billion
Defense Working Capital Funds	$8.8 Billion
Total DISA Budget	**$12.5 Billion**



Global Presence

DISA is a global organization of approximately 6,800 civilian employees; 1,500 active-duty military personnel from the Army, Air Force, Navy, and Marine Corps; and over 11,000 defense contractors. This data is as of September 2025. 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 51 percent of its people based at Fort Meade and the National Capital Region, and 49 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, Department of Defense Cyber Defense Command (DCDC), Operations and Infrastructure Center, Procurement Services

Directorate, Risk Management Executive, White House Communications Agency and Workforce Services and Development Directorate. DISA provides a core enterprise infrastructure of networks, computing centers, and enterprise services (internet-like information services) that connect 4,300 locations, reaching 90 nations supporting DoD and national interests.

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

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

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

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

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

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

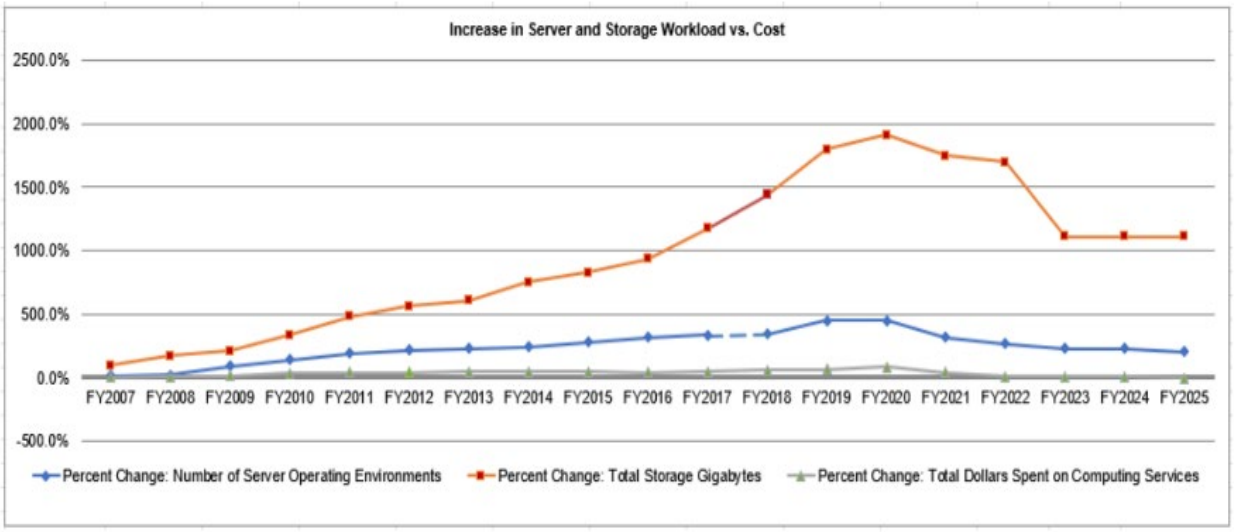
The overarching drive of the DISA Next Strategy is that DISA must: campaign; respond well in crisis, fight and win; gain and maintain relative advantage in cyberspace; and make the DoD better. This is achieved through the strategic imperatives and their coordinating operational imperatives described.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

Program Performance

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

DISA Working Capital Fund (WCF) Performance Measures

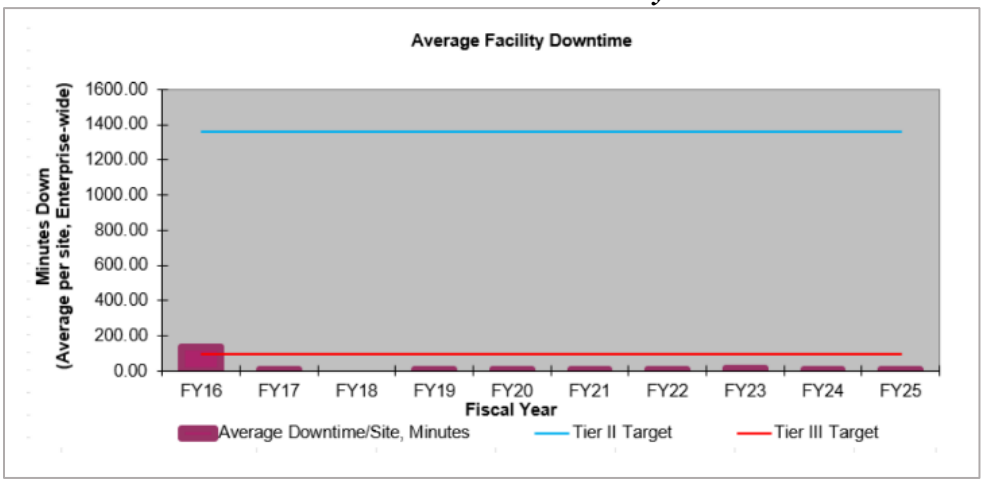
The table below represents the increased demand for DISA's server and storage computing services, which has grown significantly since FY 2007. Since that year, the number of customer driven server operating environments has increased by 202 percent, and total storage gigabytes have increased by 1,110 percent. Over the same timeframe, the cost to deliver all computing services has decreased by 4 percent. In short, customers are demanding considerably more services and are at the same time benefiting from DISA's unique ability to leverage robust computing capacity at DISA data centers.



The Computing Services (PE54) business area tracks its performance and results through the agency director's Quarterly Performance Reviews. There are two key operational metrics that are presented to the DISA director in conjunction with regular, recurring Quarterly Program Reviews. These two metrics depicted in the following tables reflect the availability of critical applications in the Core Data Centers.

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

Core Data Center Availability

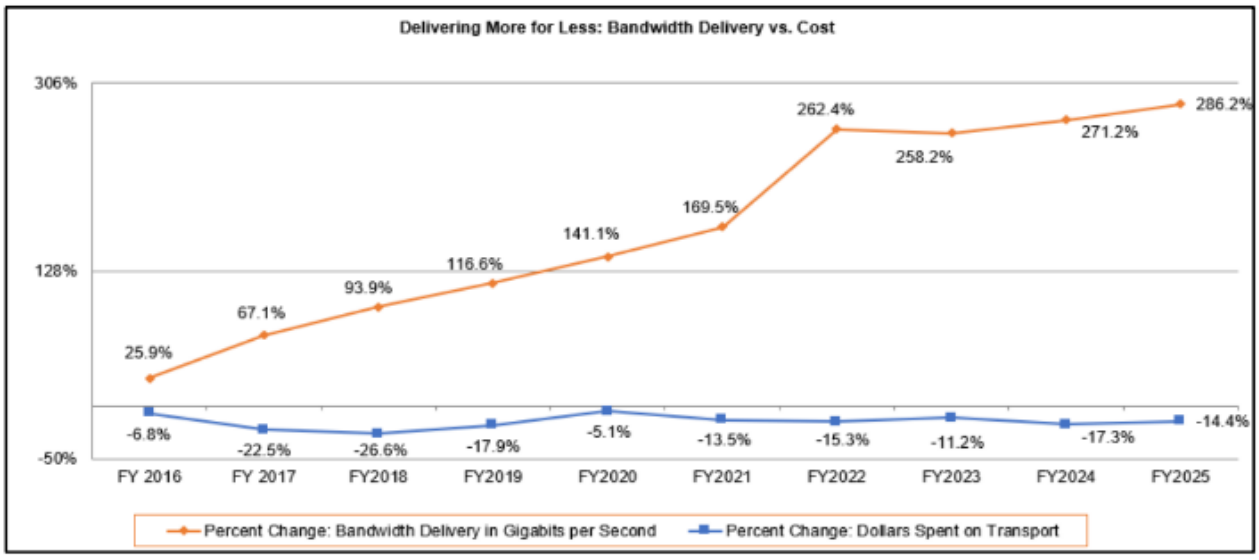


The second metric, "Capacity Service Contract Equipment Availability," represents DISA's equipment availability by technology, i.e., how well DISA is executing its responsibilities exclusive of factors outside the agency's control such as last-mile communications issues, base power outages, or the like. 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%	>99.95%	99.99%
Itanium	99.95%	>99.95%	100%
Storage	99.95%	>99.95%	99.99%
Communications Devices	99.95%	>99.95%	99.99%

The Telecommunications Services (PE55) business area provides a set of high quality, reliable, survivable, and secure telecommunications services to meet the department's command and control requirements. The major component of Telecommunications Services is the DISN, a critical element of the Department of Defense Information Network (DoDIN) that provides the warfighter with essential access to timely, secure, and operationally relevant information to ensure the success of military operations. The DISN is a collection of robust, interrelated telecommunications networks that provide assured, secure, and interoperable connectivity for the DoD, coalition partners, national senior leaders, combatant commands, and other federal agencies. Specifically, the DISN provides dynamic routing of voice, data, text, imagery (both still and full motion), and bandwidth services. The robustness of this telecommunications infrastructure has been demonstrated by DISA's repeated ability to meet terrestrial and satellite surge requirements in southwest Asia while supporting disaster relief and recovery efforts throughout the world. Overall, the DISN provides a lower customer price through bulk quantity purchases, economies of scale, and reengineering of current communication services. In spite of this continuing upward trend in demand, DISA has delivered transport services at an overall cost decrease to mission partners, as shown in the subsequent chart:



The previous chart compares the bandwidth delivery, including multiprotocol label switching connections, with transport costs. Since FY 2016, DISA has increased transport bandwidth delivery capacity 286.2 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 14.4 percent. Additionally, DISA has been able to keep these costs down without

any degradation in service. The DISN continues to meet or exceed network performance goals for circuit availability and latency, two key performance metrics.

The DISN has operating metrics tied to the department's strategic goal of information dominance. These operational metrics include the cycle time for delivery of data and satellite services as well as service performance objectives, such as availability, quality of service, and security measures. These categories of metrics have guided the development of the Telecommunication Services budget submission.

Figure 2- Major Performance and Performance Improvement Measures

SERVICE OBJECTIVE	FY 2025 Operational Goal	FY 2026 Operational Goal	FY 2027 Operational Goal
Non-Secure Internet Protocol Router Network access circuit availability	98.5%	98.50%	98.50%
Secure Internet Protocol Router Network latency (measurement of network delay) in the continental United States	<= 100 milliseconds	<= 100 milliseconds	<= 100 milliseconds
Optical Transport network availability	99.50%	99.50%	99.50%

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

Figure 3- EAS Performance Measures

SERVICE OBJECTIVE	FY 2025 Estimated ACTUAL	FY 2025 Operational Goal	FY 2026 Operational Goal*	FY 2027 Operational Goal*
Percent of total eligible contract dollars completed	73.00%	73.00%	73.00%	73.00%
Percent of total eligible contract dollars awarded to small businesses	22.00%	25.00%	20.00%	20.00%

*FY 2026 and FY 2027 goals for percent of total eligible contract dollars competed are estimates based on the released FY 2025 goal. The goals have not yet been released by the Defense Procurement Acquisition Policy (DPAP).

In addition to the program performance measures outlined above, DISA has increased accountability of its assets by linking performance standards to internal control standards. Each Senior Executive Service member at DISA has included in their performance appraisal a standard to achieve accountability of property. This standard has filtered down to managers across the agency. This increased focus on accountability for managers has had a significant impact on the critical area of safeguarding assets. DISA's AFR will be published at https://www.disa.mil/about/legal-and-regulatory/budget-and-performance-reports by Nov. 17, 2025.

Analysis of Financial Statements

BACKGROUND

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

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's Audit Committee is composed of three members who are not part of DISA. The current mission of DISA Audit Committee is to serve in an advisory role to DISA senior managers. The committee is tasked with developing, raising, and resolving matters of financial compliance and internal controls with the purpose of ensuring DISA's consistent demonstration of accurate and supportable financial reports. The committee develops and enforces guidance established for this purpose.

Defense Working Capital Fund Financial Highlights

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

Figure 4- Illustrative Table of Key Measures

(thousands)

		9/30/2025
COSTS		
Gross Program Costs	$	9,656,989
Less: Earned Revenue		(9,763,920)
Net Cost of Operations		(106,931)
NET POSITION		
Assets:		
Fund Balance with Treasury		563,518
Accounts Receivable, Net		1,013,488
Property, Plant & Equipment, Net		1,620,621
Other		1,910
Total Assets		3,199,537
Liabilities:		
Accounts Payable		907,486
Pension, Post-Employment, [& Veteran] Benefits Payable		64,453
Other Liabilities		590,181
Advances from Others and Deferred Revenue		1,916
Total Liabilities		1,564,036
Net Position (Assets minus Liabilities)	$	1,635,501

FINANCIAL POSITION

The DISA WCF reported a positive Net Position, the difference between Total Assets of $3.2 billion and Total Liabilities of $1.6 billion, on its Balance Sheet. As of Sept. 30, 2025, Net Position totaled $1.6 billion. DISA's largest asset balance is General and Right-to-Use Property, Plant, and Equipment (PP&E) at $1.6 billion or 51 percent of Total Assets followed by Intragovernmental Accounts Receivable and Fund Balance with Treasury (FBWT), representing an additional combined total of approximately $1.6 billion or 49 percent of Total Assets. Significant liabilities include Accounts Payable of $907.5 million, Other Liabilities of $590.2 million and Pension, Post-Employment, (&Veteran) Benefits Payable of $64.5 million for a combined total of approximately 100 percent of Total Liabilities.

Figure 5- Summary of Total Assets

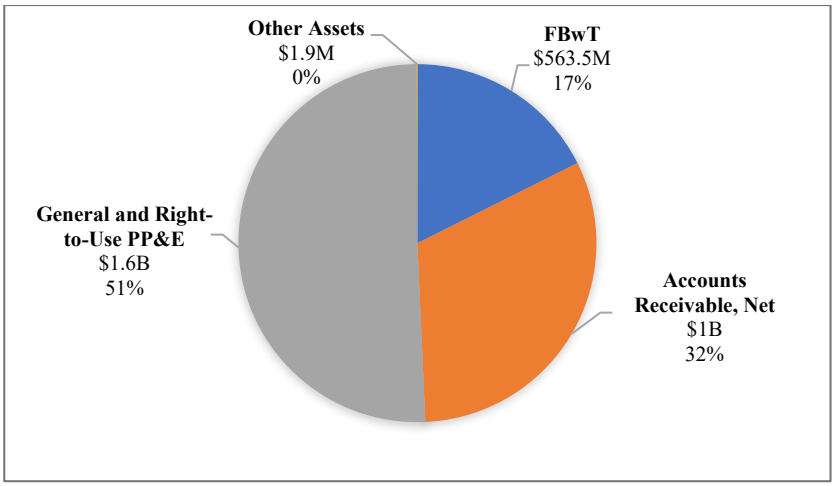


Figure 6- Summary of Total Liabilities

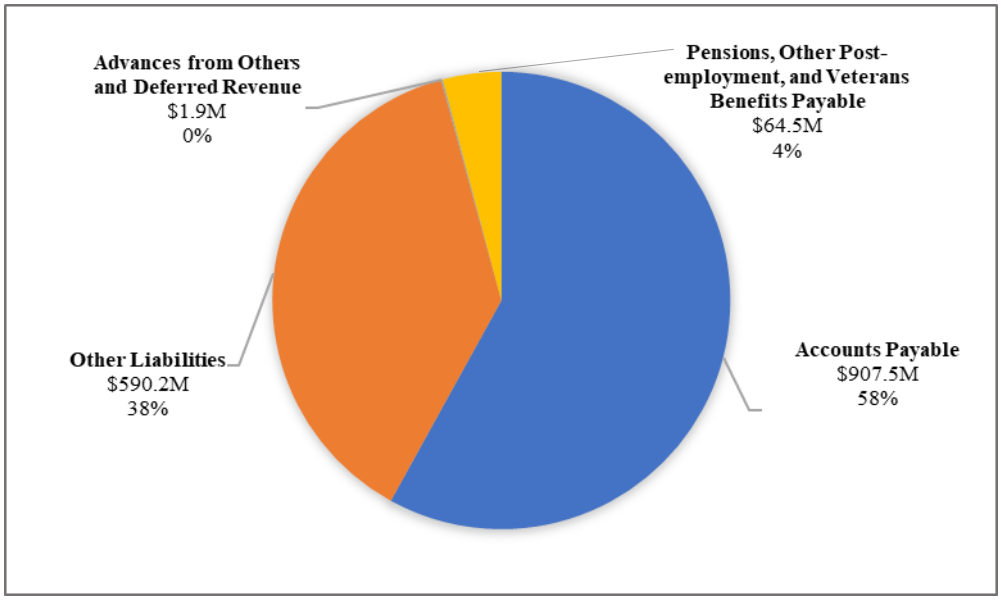
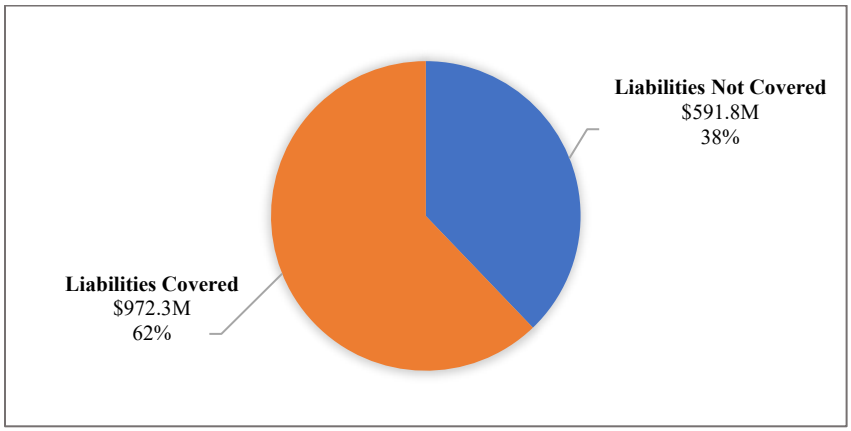


Figure 7- Liabilities Covered/Not Covered by Budgetary Resources



As of Sept. 30, 2025, $591.8 million (38 percent) of DISA WCF's liabilities were not covered by budgetary resources.

STATEMENT OF NET COST

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

Net Cost of Operations – The DISA General Fund (GF), Army, and Air Force continue to be DISA WCF's biggest customers. WCF Net Cost of Operations includes non-recoverable costs such as depreciation expense and imputed costs.

Figure 8- Net Cost of Operations

(thousands)

	2025
Gross Cost (Note 10)	$ 9,656,989
Less: Earned Revenue (Note 11)	(9,763,920)
Net Cost of Operations	$ (106,931)
Computing Services (PE54)	$ 733,580
Telecommunication Services (PE55)	2,346,662
Enterprise Acquisition Services (PE56)	6,576,747
Less: Earned Revenue	(9,763,920)
Net Cost of Operations	$ (106,931)

DISA WCF categorizes the various costs incurred during the fiscal year into three major programs:

- PE54 - The Computing Services (CS) (PE54) component of DISA's DWCF activities operates DISA data centers, which provide mainframe and server-processing operations, data storage, production support, technical services, and end-user assistance for command and control, combat support, and enterprise applications across DoD. These facilities and functions provide a robust enterprise computing environment to more than 4 million users through 17 mainframes;

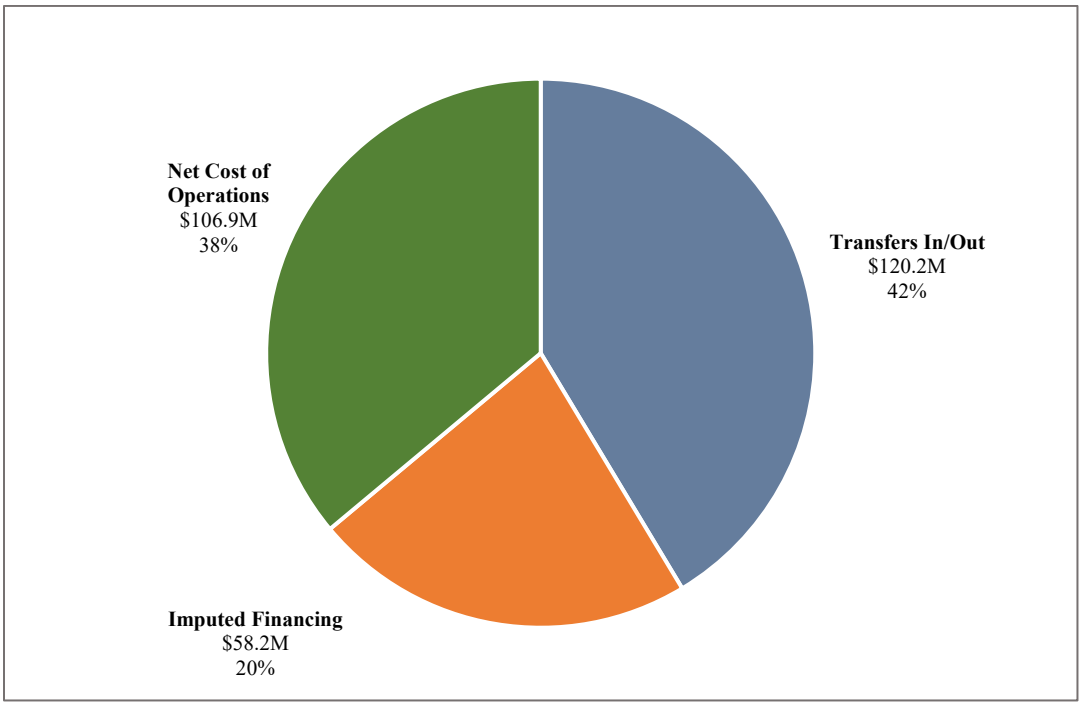
approximately 10,000 servers; 73 petabytes of storage data; 3,400 network devices and 235,000 square feet of raised floor.

- PE55 - The major element of the Telecommunication Services (PE55) component is the 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.
- PE56 - The 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.

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).

Figure 9– Statement of Changes in Net Position



STATEMENT OF BUDGETARY RESOURCES

The Statement of Budgetary Resources (SBR) presents DISA WCF's total budgetary resources, their status at the end of the period, and the relationship between the budgetary resources and the outlays made against them. In accordance with federal statutes and related regulations, obligations may be incurred and payments made only to the extent that budgetary resources are available to cover such items. The SBR 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 10- Statement of Budgetary Resources

(thousands)

	9/30/2025
One Fund	
Obligations Incurred	9,504,878
Unobligated Balances	725,320
Contract Authority	159,387
Unfilled Customer Orders	3,428,312
Net Outlays	(132,319)

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.

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.

Analysis of Systems, Controls, and Legal Compliance

Management Assurances

DISA, Office of the Chief Financial Officer (J8 -OCFO/Comptroller), has oversight of DISA's Risk Management and Internal Control (RMIC) Program. Agency assessable unit managers (AUMs) perform testing and report results for Internal Controls Over Reporting - Operations (ICOR-O) Non-Financial.

Tests and reports of results are conducted for the Internal Controls Over Reporting - Financial Systems (ICOR-FS) for the agency. In addition, the OCFO conducts testing and reports on the overall Internal Controls Over Reporting - Financial Reporting (ICOR-FR) for the agency.

Reviews, testing, and evaluations are conducted to assess if the internal control structure is compliant with the components of the Government Accountability Office (GAO) Green Book objectives of operations, reporting, and compliance. DISA's senior management has reviewed and evaluated the system of internal controls in effect during the fiscal year as of the date of this memorandum, according to the guidance in OMB Circular No. A-123 and the GAO Green Book. Included is our evaluation of whether the system of internal controls for DISA is compliant with standards prescribed by the Comptroller General.

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

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

The evaluation of internal controls extends to every responsibility and activity undertaken by DISA and applies to program, administrative, and operational controls, making adherence of RMIC not only the responsibility of management, but also every DISA employee. The concept of reasonable assurance recognizes that DISA's mission objectives are achieved, and managers must carefully consider the appropriate balance among risk, controls, costs, and benefits in our mission-support operations.

Too many controls can result in inefficiencies, while too few controls might increase risk to an unacceptable level. In that premise, errors or irregularities may occur and not be detected because of inherent limitations in any system of internal controls, including those limitations resulting from resource constraints, congressional restrictions, and other factors. Projection of any system evaluation to future periods is subject to the risk that procedures may be inadequate because of changes in conditions or that the degree of compliance with procedures may deteriorate. Therefore, this statement of reasonable assurance is provided within the limits of the preceding description.

DISA management evaluated the system of internal controls in accordance with the guidelines identified above. The results indicate that the system of internal controls of DISA, in effect as of the date of this memorandum, taken as a whole, complies with the requirement to provide reasonable assurance that the above-mentioned objectives were achieved for reporting, operations, and compliance.

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

DEFENSE INFORMATION SYSTEMS AGENCY
P. 0. BOX 549
FORT MEADE, MARYLAND 20755-0549

MEMORANDUM FOR THE OFFICE of the 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) 2025

As Director of the Defense Information Systems Agency (DISA), I recognize DISA is responsible for managing risks and maintaining effective internal controls to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act (FMFIA) of 1982. The DISA conducted its assessment of risk and internal controls in accordance with the Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control" and the Green Book, GAO-14-704G, "Standards for Internal Control in the Federal Government." This internal review also included an evaluation of the internal controls around our Security Assistance Accounts (SAA) activities. Based on the results of the assessment, the DISA can provide reasonable assurance that internal controls over operations, financial reporting, and compliance are operating effectively as of September 30, 2025. DISA's Working Capital Fund (WCF) from September 2024 through the current FY has no material weaknesses. As of July 31, 2024, there were six categories of General Funds (GF) material weaknesses (MWs) and WCF and GF significant deficiencies (SDs) that DISA is correcting or has mitigating controls in place: accounts receivable/revenue; accounts payable/expense; budgetary resources; fund balance with Treasury; financial reporting; and property, plant and equipment (PPE).

The 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. Internal reviews also included an evaluation of the internal controls around our 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, 2025.

The 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. This assessment also included an evaluation of the internal controls around our SAA activities. Based on the results of the assessment, the DISA can provide reasonable assurance that internal controls over reporting (including internal and external reporting) and compliance are operating effectively as of September 30, 2025.

The 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. This internal review also included an evaluation of the internal controls around our SAA activities. Based on the results of this assessment, DISA can provide reasonable assurance that the internal controls over the

financial systems are in compliance with the FMFIA, Section 4; Federal Financial Management Improvement Act (FFMIA), Section 803; and OMB Circular No. A-123, Appendix D, as of September 30, 2025.

DISA conducted an assessment of entity-level controls including fraud controls in accordance with the Green Book, OMB Circular No. A-123, the Payment Integrity Information Act of 2019, and GAO Fraud Risk Management Framework. In FY 2025, there has been increased focus on improper payment activity. DISA has validated that it does have an immaterial amount of improper travel payments, and the majority of improper payments identified do not have a monetary value impact. Fraud has not been identified as a contributing factor for improper payments. A corrective action plan has been put into place to mitigate travel discrepancies. 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, 2025**.**

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

If there are any questions regarding this Statement of Assurance for FY 2025, my point of contact is Mr. Justin Sponseller, at justin.c.sponseller.civ@mail.mil or (614) 692-0686.

STANTON.PAUL.TERENCE.1092476878
Digitally signed by STANTON.PAUL.TERENCE.1092476878
Date: 2025.11.06 14:48:08 -05'00'

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

Attachments:
As stated,

FY 2025 Internal Control Program Initiatives and Execution

In addition to the foundational sources of guidance such as OMB Circular A-123 and the GAO Greenbook, DISA also receives direction from and coordinates with the Office of Under Secretary of Defense Comptroller (OUSD (C)) to execute its RMIC Program. The OUSD Comptroller RMIC Team issues the FY 2025 DoD Statement of Assurance (SoA) Handbook that requires deliverables throughout the reporting cycle. The Handbook provides practical guidance to carry out the Program. There is continued emphasis on Entity Level Controls (ELCs), mitigating and closing auditor Notice of Findings and Recommendations (NFR), corrective action plan (CAP) initiation, and testing, to pave the way in support of CAP implementation. In FY 2025 remediation efforts align with the Department's overall financial statement audit objectives; however, there is more focus on integrating an Agency risk profile that identifies risks, fraud that may potentially impact the agency's strategic objective, and improper payments.

Throughout the process, DISA has provided several templates and deliverables to support not only DISA, but the overall DoD RMIC Program. During the course of the year, DISA has submitted end-to-end process control narratives and key controls; an Agency risk assessment; material weakness and deficiencies reporting and removals; an entity level control testing validation; a GAO fraud risk management (FRM) framework assessment; ICORs – FR & FS relevant systems process control narratives; ICOR – FR & FS system inventory assertion; Complementary User Entity Controls (CUEC) analysis; corrective action plans; a summary of Management's approach to internal control evaluation; and a 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 WCF has successfully closed NFRs and has no material weaknesses. DISA has made concentrated efforts for GFs to resolve and clear prior year issues and continues in its progress in strengthening its internal control structure.

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 seventeen control principles which represent fundamental elements associated with each component of control and recognizes that there are significant interdependencies among the various control principles. ELCs represent the overriding management controls that create an environment of management oversight for the financial and non-financial activities of the Department and DISA as an Agency.

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 supports NDS Strategic Priority 5: Address Institutional Management Priorities 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 continuous environment of improvement and refining processes.

The RMIC Program is managed through a three-tiered approach, which provides a structure to identify risk at an enterprise level, as well as a more granular level. The first tier, the DISA Director provides a "Tone-at-the-Top" memo which defines management's leadership and commitment towards an effective internal control structure. The second tier is supported by the Internal Control team, consisting of subject-

matter experts providing guidance and execution of the program throughout the Agency. The third tier is supported by the Assessable Unit Managers (AUMs) who manage the J-Code organizational structure within the Agency. Each Directorate's senior leadership, within each Assessable Unit (AU), collaborates with AUMs to identify areas of risks in their respective area. The coordination and consolidation of risk identifies the overall assessment of risk at the enterprise risk management level, while also reviewing DISA's detail transactions. This results in reviews and Letters of Assurance (LoAs) from each area that are integrated in the annual SoA assessment.

Oversight and Monitoring:
DISA's internal control structure of training provides assistance to AUMs; ELCs; risk assessments; continuous testing in mandatory and high-risk areas, reviews; updates and management approval of process narratives and cycle-memos; CAPs; and accountable officials LoAs are all core to an integral program of oversight and monitoring. In addition, the Senior Assessment Team (SAT) meeting occurred on August 20, 2025, providing oversight to the internal control program through discussion of results and outcomes reported in the FY 2025 SoA.

CARES Act/COVID-19:
The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed on March 2, 2020, (Public Law 116-136), to 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 of fraud, waste, and abuse is heightened when internal controls are relaxed. COVID19-related activity continues to be reviewed and tested. Operations and Maintenance funding in support of the CARES Act is canceled as of September 2025 and is in an expiring phase for research, development, testing and evaluation appropriations. There have been no laws identified that have been compromised, or major issues detected leading to fraud, waste, or abuse as validated through testing results in FY 2025.

Fraud Controls:
In FY 2025, DISA executed a fraud controls assessment on DISA's environment. The review incorporated components of GAO Fraud Risk Management Framework 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 Accountability and Transparency 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 2025, 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 from the initial testing in 2022 through the current FY 2025.

Records Management:
The DISA Records Management Team incorporates a robust records management review into its processes. The results support that DISA has established 100% 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.

Payment Integrity/ Improper Payment Recovery:
In compliance with the Payment Integrity Information Act of 2019 (Public Law 116-117, 31, United States Code § 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 (T&A), travel payments, and purchase card transactions. Controls are in place through established policy and procedures; training; separation of duties; and data mining to identify risks and fraud vulnerabilities. Additionally, the Defense Finance and Account Services (DFAS), as DISA's accounting service provider, performs overpayment recapture functions on behalf of DISA. The DFAS includes DISA transactions in their sampling populations for improper payment testing for civilian payroll and travel. In FY 2025, improper payments have been detected; however, the majority of those identified have an immaterial or no financial impact (attributable to timing of authorization and supporting documentation). A CAP has been implemented to mitigate future inconsistencies.

Key Areas for FY 2025: In continual improvement to the RMIC Program, the following areas were in focus for this FY cycle of assessment and reporting:

- Conduct verification and validation procedures on controls and processes to support closure of NFRs
- Leverage internal control activities to accelerate weakness remediation
- FMS: Incorporate control activity into narratives, policy, and processes
- Systems and Emerging Technologies: Leverage emerging technology to automate processes
- Implementation of FRM: Payment integrity for high-risk activity. Validate effective internal controls supporting visibility and alignment with GAO FRM best practices and strategy.
- Senior Officials and AUMs document and conduct oversight and monitoring efforts across respective environments.

The DISA utilizes the Committee of Sponsoring Organizations (COSO) framework principles to facilitate the flow of information between internal organizations and staff. In an effort to improve the risk and internal controls management process, DISA has developed a robust program to train individual organizations on the internal controls review process and manage internal control testing through review and assessment.

To further align the fraud risk management requirements to the GAO FRM Framework, the DISA conducts an FRM Framework Assessment.

Internal Control Structure
Using the process described below, the DISA evaluated its system of internal control and maintains sufficient documentation and an audit trail to support its evaluation and level of assurance. The DISA manages the RMIC Program through a three-tiered approach. The first tier is supported by the DISA SAT, which provides guidance and oversight to the RMIC Program. In FY 2025, the DISA Director signed a "Tone-at-the-Top" memo which defines management's leadership and commitment towards an effective RMIC program drawing attention to openness, honesty, integrity, and ethical behavior. The memo directed the Agency to follow a risk-based and results-oriented program to align with the GAO Green Book and OMB A-123. The Tone-at-the Top is established and incorporated throughout DISA by all levels of management and has a trickle-down effect to all employees.

The second tier is supported by a subject matter expert 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. The DISA provided internal control kick-off

training for the AUMs in November 2024 and conducted three additional workshops in the FY 2025 reporting cycle to address risk assessments, testing grids, and LoAs. The RMIC team compiles AU submissions for the Agency's SoA, facilitates information sharing between AUMs, consolidates results, and communicates outcomes to OUSD and agency leadership.

The third tier is supported by the AUMs, who manage at the program/Directorate level within the organization. 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 results in the AU's unique operational risks that requires evaluation.

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

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

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

Test Results:
After the tests are conducted and results are revealed, the test grid forms the basis for reporting the results in the LOA. The LOA will reflect the data reported on the test grid.

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

A. Travel (DTS):

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

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

Snapshot in Review

Internal Controls Over Reporting - Operations
Mandatory testing is required for all organizations. An AUM in coordination with senior management identifies the functions performed within their area, in addition to the required testing areas of DTS, T&A, and PP&E, to identify the level of process documentation available, and determine the associated risk of those functions. In addition, Government Purchase Card and Records Management are tested by process owners and the results of these tests are reported in each respective area's LoAs.

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 15 November each year.

DISA has not reported anti-deficiency violations in more than a decade, and we continue to demonstrate compliance with laws and regulations.

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

Additionally, DISA provides application hosting services for the Department's service providers. As a result, DISA is responsible for most of the information technology general 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.

DISA has developed and annually executes its System and Organization Controls Report (SOC 1) CUEC review and documentation processes which is outlined in the Agency's "SOC 1 Report and CUEC Review" Standard Operating Procedures (SOP). In accordance with this process, DISA executes the following activities:

- Monitors and communicates with its service providers to understand the status of their annual Statement on Standards for Attestation Engagements (SSAE) 18 examinations and identifies anticipated changes to the services or controls they perform, CUECs, and any other relevant content in their respective SOC 1 reports;
- Performs a risk assessment to identify service providers that are relevant to financial reporting; reviews all SOC 1 reports issued by relevant service organizations and subservice organizations to assess and document the effectiveness of their SOCs and the impact to DISA's financial reporting;
- Assesses the CUECs listed in each SOC 1 report; and documents and tests DISA's controls that correspond to each relevant CUEC.

DISA performs annual testing to evidence the design, implementation, and operating effectiveness of these CUECs, based on our risk assessment of each relevant CUEC. For CUECs determined to be common across multiple systems or SOC 1 reports (i.e. "common CUECs"), testing is performed every year for those assessed as high risk. DISA also tests lower risk common CUECs each year, in accordance with the testing schedule that is based on our risk assessment. In addition, DISA has expanded testing of non-common CUECs, using a phased approach for a subset of service organizations each year, and prioritizing selected controls based on our risk assessment. Using this defined process, DISA continues to make substantial progress toward evidencing the implementation of relevant CUECs, in support of the Secretary of Defense audit priorities.

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 mission specific key 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 and 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.

Summary of Internal Control Evaluation Approach: DISA's approach to internal controls extends to all responsibilities and activities undertaken within DISA. The 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.

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 2025, DISA continued to operate, enhance, and sustain the Financial Accounting and Management Information System (FAMIS), which supports the full breadth of DISA's WCF lines of business. The FAMIS-WCF solution provided DISA with DoD Standard Line of Accounting and USSGL compliance in support of a clean audit opinion for the WCF. Additionally, FAMIS deployed the first phase of the future state compliant telecom Business Enterprise Architecture (BEA) solution. This solution enables DISA to begin the sunset activity of legacy telecom systems and provides a compliant and automated solution that complies with DoD policies. FAMIS continued to maintain a strong security posture, receiving a 3-Year Authority to Operate (ATO). Additional capabilities and modernizations deployed into FAMIS included enhanced automation and reconciliation of core cash matching functionalities, enabling DISA's WCF to maintain its record of zero unmatched disbursements.

DISA migrated its GF accounting system solution out of the Defense Agencies Initiative (DAI) solution and into FAMIS in FY 2025. The implementation of FAMIS as a Service (FaaS) across both DISA's WCF and GF improves operational efficiencies, ensures data integrity, and supports compliance of financial standards while leveraging the capabilities of the existing FAMIS baseline. Go-live operational capability for DISA's GF occurred in October 2024. Finally, FAMIS began laying the groundwork to migrate to a commercial cloud environment.

In addition to the accounting system, DISA's financial system's 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 GF and DWCF funds through static reports, interactive data cubes, and customizable dashboards.

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

In that regard, DISA continues to standardize the customer order provisioning process to include a single integrated order entry solution for all orders while validating the solutions that integrate with DISA's financial and contracting systems and tools. DISA's financial systems strategy is purpose driven to continually innovate and increase its use of technologies, such as robotic process automation and artificial intelligence, to improve and automate financial and contractual transactions. As a result of DISA's experience using its newly modernized/compliant accounting systems for the previous five years, its accounting operations have stabilized, and it is taking

advantage of its capabilities to improve accounting processes and audit readiness, and to set the course for further financial modernization efforts across its business ecosystem. This includes identifying and assessing opportunities to sunset older legacy supporting systems by consolidating and/or migrating functionality to more modern and flexible technologies and architectures.

One example of this modernization is the current undertaking to accredit and stand up a new financial system called the DISA Integrated Management and Execution System (DIMES). DIMES is an Enterprise Performance Management (EPM) solution based on the OneStream platform that supports budgeting, forecasting, financial reporting, and data quality management. DISA implemented the budget execution phase of the project in FY 2025 supporting spend planning; subsequent phases to include budget formulation and reporting will be kicked off in FY 2026. Once completed, DIMES will be the single platform for users to access budget formulation and execution data for both the GF and WCF and as such, will replace DFMS and DBS (DISA Financial Management System and DWCF Budgeting System).

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

Forward-Looking Information

The DoD is undergoing an IT environment transformation, aiming to converge communications, computing, and enterprise services into a unified joint platform that can be leveraged for all department missions. DISA is at the forefront of this evolution, uniquely positioned to deliver enterprise solutions through the development, integration, and synchronization of technical plans, programs, and capabilities. This presents both significant opportunities and critical risks that must be managed by DISA.

Opportunities: DISA expects the following opportunities to yield long-term financial benefits and contribute to overall budgetary efficiency.

- **Modernized Infrastructure and Services:** DISA can drive modernization with initiatives like:
    - **Defense Enterprise Office Solutions (DEOS):** A commercially provided, cloud-based enterprise service for common communication, collaboration, and productivity services, leading to the decommissioning of legacy email, video, and audio-conferencing services.
    - **Fourth Estate Network Optimization:** This PE55 reform initiative converges DoD networks, service desks, and operations centers into a consolidated, secure, and effective environment.
    - **Joint Warfighting Cloud Capability (JWCC):** This PE56 multiple award contract vehicle provides the DoD with direct access to multiple Cloud Service Providers (CSPs) to acquire commercial cloud capabilities and services at the speed of mission – at all classification levels, from headquarters to the tactical edge. Direct awards with the CSPs also allows for streamlined provisioning of cloud services, fortified security, and commercial pricing parity.
- **Cloud Leadership:** By delivering an on-premises, cloud hosting capability and commercial cloud access infrastructure, DISA can reduce the data center footprint, streamline cybersecurity, and provide warfighters with access to data when and where it is needed. This includes the transition of network management tools to the commercial cloud, modernizing the management and efficiency of the network backbone.

- **Optimized Computing Services:** The Compute Operations model (formerly Ecosystem) supports computing services for mission partners worldwide by aligning like-functions across a single computing enterprise and establishing a unified computing structure operating under a single command (one large virtual data center). This model prioritizes excellence in service delivery, process efficiency, and standardization for tools and processes. These optimization efforts have already yielded savings of $717 million over 10 years.

However, realizing these opportunities hinge on effectively mitigating critical risks associated with DISA's strategic imperatives.

Significant Risks: DISA has determined the following risks would likely negatively impact financial results if left unaddressed:

- **Compromised Mission Effectiveness & Competitive Disadvantage:** Failure to provide relevant, modern enterprise and business tools will hinder Combatant Commands (CCMDs), Military Departments (MILDEPs), and Defense Agencies and Field Activities (DAFAs), resulting in a competitive disadvantage and vulnerability to cyberattacks. Outdated tools create inefficiencies and impede the ability to adapt to emerging threats.
- **Service Disruptions and Data Integrity Issues:** Failure to maintain a resilient and secure DISN backbone could lead to service disruptions, compromised data integrity, and increased vulnerability to attacks, hindering mission-critical applications and situational awareness.
- **Delayed Decision-Making & Compromised Cyber Defense:** Failure to operationalize data could lead to a lack of situational awareness, delayed decision-making, and an inability to effectively defend against cyber threats. This includes outdated policies, reduced compliance, and ineffective threat mitigation.
- **Siloed Networks & Inconsistent Security:** Failure to unify the network could result in inconsistent security postures, increased complexity, limited interoperability, and missed opportunities for cost savings.
- **Increased Vulnerabilities & Higher Costs:** Failure to divest technical debt will likely lead to increased security vulnerabilities, higher maintenance costs, reduced performance, and the diversion of resources from critical modernization efforts.

DISA must continue to address these risks, while capitalizing on the opportunities presented by the DoD's IT transformation. By prioritizing the strategic imperatives of operating and securing the DoDIN, supporting Command, Control, and Communications (C3), optimizing the network, and operationalizing data, DISA can ensure that the Department of Defense remains secure, effective, and adaptable in a rapidly evolving threat landscape.

Defense Information Systems Agency
Working Capital Fund
Principal Statements
Fiscal Year 2025, Ending Sept. 30, 2025

Department of Defense
Defense Information Systems Agency WCF
Balance Sheet
As of Sept. 30, 2025
($ in thousands)

Figure 11- Balance Sheet

		2025
Intragovernmental assets:		
Fund Balance with Treasury (Note 2)	$	563,518
Accounts Receivable, Net (Note 3)		1,012,382
Total Intragovernmental Assets		1,575,900
Other than Intragovernmental Assets:		
Accounts Receivable, Net (Note 3)		1,106
Property, Plant and Equipment, net (Note 4)		1,620,621
Advances and Prepayments		1,910
Total Other than Intragovernmental Assets		1,623,637
Total Assets	$	3,199,537
Liabilities (Note 7)		
Intragovernmental Liabilities:		
Accounts Payable	$	20,619
Advances from Others and Deferred Revenue		1,910
Other Liabilities (Notes 7 and 9)		4,080
Total Intragovernmental Liabilities		26,609
Other than Intragovernmental Liabilities:		
Accounts Payable		886,867
Federal Employee Salary, Leave, and Benefits Payable (Note 6)		59,891
Pension, Post-Employment, and Veteran Benefits Payable (Note 6)		4,562
Advances from Others and Deferred Revenue		6
Other Liabilities (Notes 7, 8, and 9)		586,101
Total Other than Intragovernmental Liabilities		1,537,427
Total Liabilities		1,564,036
Commitments and Contingencies (Note 9)		
Net Position:		
Cumulative Results of Operations		1,635,501
Total Cumulative Results of Operations (Consolidated)		1,635,501
Total Net Position		1,635,501
Total Liabilities and Net Position	$	3,199,537

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

Department of Defense
Defense Information Systems Agency WCF
Statement of Net Cost
As of Sept. 30, 2025
($ in thousands)

Figure 12- Statement of Net Cost

Gross Program Costs (Note 10, Note 13)		**2025**
Gross Costs (Note 10)	$	9,656,989
Less: Earned Revenue (Note 11)		(9,763,920)
Net Cost of Operations	$	(106,931)
Computing Services (PE54)	$	733,580
Telecommunications Services (PE55)		2,346,662
Enterprise Acquisition Services (PE56)		6,576,747
Less: Earned Revenue		(9,763,920)
Net Other Program Costs:		(106,931)
Net Cost of Operations:	$	(106,931)

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

Department of Defense
Defense Information Systems Agency WCF
Statement of Change in Net Position
As of Sept. 30, 2025
($ in thousands)

Figure 13- Statement of Changes in Net Position

CUMULATIVE RESULTS OF OPERATIONS	2025
Beginning Balance	$ 1,350,192
Transfers In/Out Without Reimbursement	120,193
Imputed Financing	58,185
Net Cost of Operations	(106,931)
Net Change in Cumulative Results of Operations	285,309
Total Cumulative Results of Operations	1,635,501
Net Position	$ 1,635,501

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

Department of Defense
Defense Information Systems Agency WCF
Statement of Budgetary Resources
As of Sept. 30, 2025
($ in thousands)

Figure 14- Statement of Budgetary Resources

		2025
Budgetary Resources		
Unobligated Balance from Prior Year Budget Authority, Net (Note 12)	$	610,760
Contract Authority (Discretionary and Mandatory)		159,387
Spending Authority from Offsetting Collections (Discretionary and Mandatory)		9,460,051
Total Budgetary Resources	$	10,230,198
Status of Budgetary Resources		
New Obligations and Upward Adjustments (Total)	$	9,504,878
Unobligated Balance, End of Year		
Apportioned, Unexpired Accounts		725,320
Unexpired Unobligated Balance, End of Year		725,320
Unobligated Balance, End of Year (Total)		725,320
Total Budgetary Resources	$	10,230,198
Outlays, Net		
Outlays, Net (Total) (Discretionary and Mandatory) (Note 13)	$	(132,319)
Agency Outlays, Net (Discretionary and Mandatory)	$	(132,319)

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

Defense Information Systems Agency
Working Capital Fund
Notes to the Principal Statements
Fiscal Year 2025, Ending Sept. 30, 2025

Note 1. Reporting Entity and Summary of Significant Accounting Policies

1A. Reporting Entity

Defense Information Systems Agency (DISA), a combat support agency within the Department of Defense (DoD), is a component reporting entity, as defined by the Statement of Federal Financial Accounting Standards (SFFAS) 47, and its financial statements are consolidated into those of the DoD. These financial statements outline key funding for a component of the U.S. government. Some assets and liabilities can be offset by a different entity, thereby eliminating it from government-wide reporting.

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

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

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

1B. Accounting Policies

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

DISA records accounting transactions on both an accrual and budgetary basis of accounting. Under the accrual method, revenue is recognized when earned and costs/expenses are recognized when incurred, without regard to receipt or payment of cash. Budgetary accounting facilitates compliance with legal constraints and controls over the use of federal funds. DISA WCF presents the Balance Sheet, Statement of Net Cost, and Statement of Changes in Net Position which is a summation of the components less the eliminations. The Statement of Budgetary Resources is a summary of the DoD components and presented on a combined basis. Under the Statement of Budgetary Resources, intragovernmental activity has not been eliminated. The intra-DISA WCF balances for outlays and collections business between the Telecommunication Services Enterprise Acquisition Services (TSEAS) and Computing Services (CS) business components have been removed from the Statement of Budgetary Resources (SBR).

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

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

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

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

4) *Technical Bulletin 2020-1*: *Loss Allowance for Intragovernmental Receivables*. Issued Feb. 20, 2020; Effective upon issuance.

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

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 the Department of the Treasury (Treasury) accounts. The disbursing offices of the DFAS, the military departments, the U.S. Army Corps of Engineers (USACE), and the Department of State's financial service centers process majority of the DoD's cash collections, disbursements, and adjustments worldwide. Each disbursing station reports to Treasury on checks issued, electronic fund transfers, interagency transfers, and deposits.

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

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

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

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

DISA Working Capital Fund FBWT balance is reconciled monthly to the amounts reported in the Cash Management Report (CMR), which represents DISA's portion of the FBWT balance reported by the Treasury Department.

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, 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, 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

As required for all significant reporting entities by OMB Circular A-136, for FY 2025, single-year statements should be presented.

1G. Classified Activities

Accounting standards require all reporting entities to disclose that accounting standards allow certain presentations and disclosures to be modified, if needed, to prevent the disclosure of classified information.

1H. Standardized Balance Sheet, the Statement of Changes in Net Position and Related Footnotes – Comparative Year Presentation

The format of the Balance Sheet has changed to reflect more detail for certain line items, as required for all significant reporting entities by OMB Circular A-136. This change does not affect totals for assets, liabilities, or

net position and is intended to allow readers of this Report to see how the amounts shown on the DoD-wide Balance Sheet are reflected on the Government-wide Balance Sheet, thereby supporting the preparation and audit of the Financial Report of the United States Government. The mapping of U.S. Standard General Ledger (*USSGL)* accounts, in combination with their attributes, to particular Balance Sheet lines and footnotes is directed by the guidance published periodically under TFM, USSGL Bulletins, *Section V*. The footnotes affected by the modified presentation are *Federal Employee and Veteran Benefits Payable*, *Other Liabilities*, and *Reconciliation of Net Cost to Net Outlays*.

Effective in FY 2024, the presentation of the Statement of Net Cost has changed to align with the Department's new definition of major programs. Office of Management and Budget *Circular No. A-136* states that the Statements of Net Cost must present the net cost of operations by an agency's defined major programs. As such, the Department updated their major programs. See *Suborganization Program Costs* for further information.

Note 2. 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 $725.3 million represents the cumulative amount of budgetary authority set aside to cover future obligations and is not restricted for future use. The available balance consists primarily of the unexpired, unobligated balance that has been apportioned and available for new obligations.

Obligated balance not yet disbursed in the amount of $4.5 billion represents funds obligated for goods and services but not paid.

The non-FBWT budgetary accounts in the amount of $4.6 billion reduce budgetary resources and are primarily composed of unfilled customer orders without advance from customers in the amount of $3.4 billion, contract authority in the amount of $176.6 million, receivables and other in the amount of $1 billion.

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 15- Fund Balance with Treasury

(thousands)

DISA WCF	2025
Unobligated Balance	$ 725,320
Obligated Balance not yet Disbursed	4,462,065
Non-FBWT Budgetary Accounts:	
Unfilled Customer Orders without Advance	(3,428,312)
Unfunded Contract Authority	(176,643)
Receivables and Other	(1,018,912)
Total Non-FBWT Budgetary Accounts	(4,623,867)
Total FBWT	$ 563,518

Note 3. Accounts Receivable, Net

Accounts receivable represents 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 16- Accounts Receivable, Net

(thousands)

DISA WCF 2025	Gross Amount Due	Allowance for Estimated Uncollectibles	Accounts Receivable, Net
Intragovernmental Receivables	$ 1,018,913	$ (6,531)	$ 1,012,382
Non-Federal Receivables (From the Public)	1,270	(164)	1,106
Total Accounts Receivable	$ 1,020,183	$ (6,695)	$ 1,013,488

Note 4. Property, Plant, and Equipment, Net

DISA WCF general Property, Plant, and Equipment (PP&E) is composed of telecommunications and computing services with related equipment, software, construction-in-progress, and right-to-use lease assets with a net book value (NBV) of $1.6 billion.

DISA WCF PP&E consists of telecommunications equipment, computer equipment, computer software, right-to-use lease assets, and construction in progress, whereby the acquisition cost falls within prescribed thresholds and the estimated useful life is two or more years. PP&E assets acquired prior to Oct. 1, 2013, were capitalized at prior threshold levels ($100 thousand for equipment and $250 thousand for real property). PP&E with an acquisition cost of less than the capitalization threshold is expensed when purchased. Property and equipment meeting the capitalization threshold is depreciated using the straight-line method over the initial or remaining useful life as appropriate, which can range from three to 30 years. Per SFFAS 54, right-to-use asset thresholds are left to the discretion of the agency. DISA has established a right-to-use threshold of $32.5 thousand for FY 2025. DISA WCF will expense leases with

a right-to-use asset balance below $32.5 thousand.

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

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 fiscal year.

Figure 17- General Property, Plant, and Equipment, Net

(thousands)

DISA WCF	2025
General PP&E, Net Beginning of Year	$ 1,486,977
Balance Beginning of Year, Adjusted	1,486,977
Capitalized Acquisitions	180,476
Right-to-Use Lease Assets	262,057
Amortization of Right-to-Use Lease Assets	(186,079)
Dispositions	(18,413)
Transfers in/(out) without Reimbursement	120,193
Depreciation Expense	(224,590)
Balance End of Year	$ 1,620,621

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

Figure 18- Major General PP&E Asset Classes

(thousands)

DISA WCF 2025 Major Asset Classes	Depreciation/ Amortization Method	Service Life	Acquisition Value	(Accumulated Depreciation/ Amortization)	Net Book Value
Internal Use Software	S/L	2-5 or 10	$ 232,169	$ (201,154)	$ 31,015
General Equipment	S/L	Various*	2,719,997	(1,925,011)	794,986
Right-to-Use Lease Asset	S/L	Lease term	1,261,293	(571,254)	690,039
Construction-in-Progress	N/A	N/A	104,581	N/A	104,581
Total General PP&E			$ 4,318,040	$ (2,697,419)	$ 1,620,621

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

*PE55 and PE56 use 5 years for depreciation and PE54 uses 3 years for most depreciation, unless otherwise specified (35/40/45 years). DISA follows the FMR Vol. 4 Ch. 25 Table 25-2 for useful life unless specifically stated in contract documents.

Note 5. Liabilities Not Covered by Budgetary Resources

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

Intragovernmental liabilities-other is composed of DISA WCF's unfunded Federal Employees' Compensation Act (FECA) liability in the amount of $1.1 million. These liabilities will be funded in future periods.

Other than intragovernmental liabilities-federal employee benefits payable consists of various employee actuarial liabilities not due and payable during the current fiscal year. As of Sept. 30, 2025, DISA WCF's liabilities consist of federal employee and veteran benefits payable in the amount of $4.6 million and Other Liabilities in the amount of $586.1 million. Other liabilities consist of unfunded lease liability. These liabilities will be funded in future periods.

Starting in FY 2024, Federal agencies are required to report a right-to-use asset and a corresponding lease liability for material non-intragovernmental, no-short-term contracts when the reporting entity has the right to control access to and obtain benefits from the use of real property, equipment, or other PP&E. The Department had $584.6 million of uncovered lease liabilities in FY 2025.

Figure 19- Liabilities Not Covered by Budgetary Resources

(thousands)

DISA WCF	2025
Intragovernmental Liabilities	
Other	$ 1,089
Total Intragovernmental Liabilities	1,089
Other than Intragovernmental Liabilities	
Pension, Post-Employment, and Veterans Benefits Payable	4,562
Other Liabilities	586,101
Total Other than Intragovernmental Liabilities	590,663
Total Liabilities Not Covered by Budgetary Resources	591,752
Total Liabilities Covered by Budgetary Resources	972,284
Total Liabilities	$ 1,564,036

Note 6. Federal Employee and Veterans Benefits Payable

Expense Components

For FY 2025, the only expense component pertaining to other actuarial benefits for DISA WCF is the FECA expense. The Department of Labor (DOL) provides the expense data to DISA. The staffing ratio data from DISA headquarters determines the allocation of the expense to DISA WCF.

DOL provided an estimate for DISA's future workers' compensation benefits of $8.6 million in total, of which $4.6 million was distributed to DISA WCF based upon staffing ratios. DISA made the distribution using DISA's normal methodology of apportioning FECA liability to WCF based upon relative staffing levels. DISA used the same apportionment methodology in prior years.

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

Changes in Actuarial Liability

Fluctuations in the total liability amount charged to DISA by DOL will cause changes in FECA liability. FECA liability, which falls under other actuarial benefits, decreased $139.3 thousand due to fluctuations in Cost of Living Adjustments (COLA) and Consumer Price Index Medical (CPI-M) inflation factors that in turn adjusted the actuarial liability estimate provided by DOL (http://www.dol.gov/ocfo/publications.html).

Figure 20- Federal Employee and Veterans Benefits Payable

(thousands)

DISA WCF 2025	Liabilities	(Assets Available to Pay Benefits)	Unfunded Liabilities
Other Benefits			
FECA	$ 4,562	$ -	$ 4,562
Total Other Benefits	4,562	-	4,562
Federal Employee Benefits Payable	4,562	-	4,562
Federal Employee Salary, Leave, and Benefits Payable	59,891	(59,891)	-
Other Benefit-Related Payables included in Intragovernmental Other Liabilities	4,080	(2,990)	1,090
Total Federal Employee Benefits Payable	$ 68,533	$ (62,881)	$ 5,652

Note 7. Other Liabilities

Intragovernmental

Federal Employee and Veteran Benefits Payable: $4.1 million. This represents liabilities for pensions, Other Retirement Benefits (ORB), and Other Post Employment Benefits (OPEB) (including post-retirement health, life insurance, veterans' compensation and burial, and veteran education benefits).

Other Than Intragovernmental

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

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

Figure 21- Other Liabilities

(thousands)

DISA WCF 2025	Current Liability	Non-Current Liability	Total
Intragovernmental Other Liabilities			
Other Liabilities	$ 3,491	$ 589	$ 4,080
Total Intragovernmental Other Liabilities	3,491	589	4,080
Other than Intragovernmental Other Liabilities			
Contingent Liabilities	-	1,480	1,480
Right-to-Use Lease Liability	-	584,621	584,621
Total Other than Intragovernmental Other Liabilities	-	586,101	586,101
Total Other Liabilities	$ 3,491	$ 586,690	$ 590,181

Note 8. Leases

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

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

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

Effective October 1, 2024, DISA WCF established a $32,500 capitalization threshold for leases following a materiality assessment of its right-to-use asset data that was applied to the population retrospectively. Leases below this value are now expensed rather than capitalized, resulting in the removal of 1,232 leases and a corresponding reduction of $22.7 million in right-to-use assets. DISA WCF now presents only those leases considered materially significant. See PP&E note for additional property information.

As of Sept. 30, 2025, DISA is recognizing a total of 3,862 right-to-use assets, which include telecommunication, commercial space, office equipment and fiber optic cables. These leasing arrangements have terms from 2 to 9 years. Among these, DISA currently holds 187 lease agreements denominated in foreign currencies, including the Euro, British Pound Sterling, Bahraini Dinar, Turkish Lira, and Kuwaiti Dinar. The corresponding lease liabilities and right-to-use assets have been converted to U.S. dollars using exchange rates effective as of Sept. 30, 2025.

Land and Building Leases

As of Sept. 30, 2025, DISA WCF operates in 18 locations, of which 17 sites are located on property (primarily military bases) where no rent is charged and only utilities are required. The one remaining site is located on commercial property and covered under a long-term real estate lease expiring in 2028. The General Services Administration acquires and manages commercial property leases on behalf of the federal government; therefore, this lease is considered intragovernmental. This lease generally requires DISA WCF to pay property taxes, utilities, security, custodial services, parking, and operating expenses. Certain leases contain renewal options. The annual lease expense for the building lease in FY 2025 is $755.7 thousand.

In addition, DISA WCF currently has two non-federal, long-term lease arrangements, each with a five-year lease term.

Equipment Leases

DISA WCF currently leases 131 photocopiers within two agreements and 18 vehicles within one agreement located across various sites. The photocopiers are leased for three years, while the vehicles are leased for one year with an annual renewal option. The annual lease expense for the equipment leases in FY 2025 is $471.1 thousand.

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

Other Leases
DISA WCF maintains two non-federal, long-term lease arrangements. One arrangement pertains to data centers located in Miami, FL, and Culpeper, VA, with a five-year lease term. The other arrangement consists of a ground facility agreement that supports bandwidth services and remains in effect for four years.

The following table provides the current right-to-use asset cost and accumulated amortization as of Sept. 30, 2025, for leases other than (1) short-term leases, (2) contracts or agreements that transfer ownership, and (3) intragovernmental agreements:

Figure 22-Right-to-Use Asset Net Book Value

(thousands)

RTUA	Accumulated Amortization	Net Book Value (RTUA – A/A)
$ 1,261,293	$ 571,254	$ 690,039

The following table provides future lease payments, as of Sept. 30, 2025, for leases other than (1) short-term leases, (2) contracts or agreements that transfer ownership, and (3) intragovernmental agreements:

Figure 23- Future Payments Right-to-Use Leases

(thousands)

DISA WCF 2025				
Principal				
	Land and Buildings	**Equipment**	**Other**	**Total**
Fiscal Year				
2026	$ 3,593	$ 4	$ 170,406	$ 174,003
2027	2,973	-	108,687	111,660
2028	2,016	-	100,252	102,268
2029	824	-	64,120	64,944
2030	-	-	54,377	54,377
2031-2035	-	-	77,370	77,370
2036 and After	-	-	-	-
	$ 9,406	$ 4	$ 575,212	$ 584,622
Interest				
	Land and Buildings	**Equipment**	**Other**	**Total**
Fiscal Year				
2026	$ 359	$ -	$ 20,021	$ 20,380
2027	197	-	14,465	14,662
2028	87	-	10,253	10,340
2029	18	-	6,840	6,858
2030	-	-	4,400	4,400
2031-2035	-	-	3,047	3,047
2036 and After	-	-	-	-
	$ 661	$ -	$ 59,026	$ 59,687
Total				
	Land and Buildings	**Equipment**	**Other**	**Total**
Fiscal Year				
2026	$ 3,953	$ 4	$ 190,427	$ 194,384
2027	3,169	-	123,152	126,321
2028	2,103	-	110,505	112,608
2029	842	-	70,960	71,802
2030	-	-	58,777	58,777
2031-2035	-	-	80,417	80,417
2036 and After	-	-	-	-
	$ 10,067	$ 4	$ 634,238	$ 644,309

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

Figure 24- Interest Rate Range

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

DISA WCF currently has 2,870 (28 short-term and 2,842 long-term) intragovernmental lessor arrangements. Below is a table of future lease payments that are to be received from other federal agencies:

Figure 25- Future Payments Intragovernmental Leases

(thousands)

DISA WCF 2025	Asset Category			
	Land and Buildings	Equipment	Other	Total
1. Federal				
Fiscal Year				
2026	$ 1,003	$ 4	$ 71,811	$ 72,818
2027	924	-	51,636	52,560
2028	970	-	46,517	47,487
2029	842	-	42,705	43,547
2030	-	-	35,808	35,808
2031-2035	-	-	41,370	41,370
2036 and After	-	-	-	-
Total Intragovernmental Future Lease Payments	$ 3,739	$ 4	$289,847	$293,590

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

Note 9. Commitments and Contingencies

DISA WCF may be a party in various administrative proceedings and legal actions related to claims for environmental damage, equal opportunity matters, and contractual bid protests. DISA WCF reviews the agency claims report and determines if a liability should be recorded for the reporting period. DISA WCF recorded a $1.5 million contingent liability for the fourth quarter of FY 2025. While this liability has been settled, the payout is pending. The individual claim amounts did not meet the threshold for inclusion in the legal representation letter.

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 (PE54, PE55 and PE56) administered by a responsible reporting entity. The PE54, PE55 and PE56 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 disclose 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 the 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 26- 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	2025
One Fund				
Gross Costs	$ 9,345,926	$ 348,438	$ -	$ 9,694,364
Less earned revenues	(953)	(9,762,967)	-	(9,763,920)
Net Costs	9,344,973	(9,414,529)	-	(69,556)
Component Level				
Gross Costs	-	-	(37,375)	(37,375)
Less earned revenues	-	-	-	-
Net Costs	-	-	(37,375)	(37,375)
Net Cost of Operations				
Gross Costs	9,345,926	348,438	(37,375)	9,656,989
Less Total Revenues	(953)	(9,762,967)	-	(9,763,920)
Total Net Costs	$ 9,344,973	$ (9,414,529)	$ (37,375)	$ (106,931)

Figure 27- Net Cost of Operations

(thousands)

Net Cost of Operations			2025
	Gross Cost	Earned Revenue	Net Cost of Operations
Computing Services (PE54)	$ 733,580	(822,367)	$ (88,787)
Telecommunication Services (PE55)	2,346,662	(2,718,289)	(371,627)
Enterprise Acquisition Services (PE56)	6,576,747	(6,223,264)	353,483
Total Gross Cost	$ 9,656,989	(9,763,920)	$ (106,931)

Note 11. Exchange Revenues

DISA WCF reports exchange revenue 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. The 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 undersecretary 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, 2025, DISA WCF incurred $9.5 billion in obligations, all of which are reimbursable and none of which are exempt from apportionment.

The total unobligated balance available (Apportioned) as of Sept. 30, 2025, is $725.3 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 Regulation (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, 2025, DISA WCF's net amount of budgetary resources obligated for undelivered orders is $3.5 billion.

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

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

Figure 28- Net Adjustments to Unobligated Balance Brought Forward, October 1

(thousands)

DISA WCF	2025
Unobligated balance brought forward, October 1	$ 610,760
Recoveries of prior year unpaid obligations	9,604
Unobligated balance of contract authority withdrawn	(9,604)
Unobligated Balance from Prior Year Budget Authority, Net (Discretionary and Mandatory)	$ 610,760

DISA WCF had adjustments to the balance brought forward, October 1. This includes $9.6 million in recoveries of prior period unpaid obligations and a decrease of $9.6 million in unobligated balance of contract authority withdrawn.

Figure 29- Budgetary Resources Obligated for Undelivered Orders at the End of the Period

(thousands)

	2025
Intragovernmental	
Unpaid	$ 79,547
Total Intragovernmental	79,547
Other Than Intragovernmental	
Unpaid	3,412,150
Prepaid/Advanced	1,910
Total Other Than Intragovernmental	3,414,060
Total Budgetary Resources Obligated for Undelivered Orders at the End of the Period	$ 3,493,607

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 is 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. The Unreconciled difference of $(1) is due to rounding.

Figure 30- Reconciliation of the Net Cost of Operations to Net Outlays

(thousands)

DISA WCF	Intragovernmental	With the Public	Total
Net Cost (Revenue) reported on SNC	$ (9,425,902)	$ 9,318,971	$ (106,931)
Components of Net Cost Not Part of Net Outlays:			
Property, plant, and equipment depreciation expense	-	(224,590)	(224,590)
Property, plant, and equipment disposals & revaluations	-	101,780	101,780
Lessee Lease Amortization	-	(186,079)	(186,079)
Increase/(Decrease) in Assets:			
Accounts receivable, net	154,071	(473)	153,598
Advances and Prepayments	-	(90)	(90)
(Increase)/decrease in liabilities:			
Accounts Payable	17,097	(57,060)	(39,963)
Lessee Lease Liability	-	177,412	177,412
Federal employee salary, leave, and benefits payable	-	(7,593)	(7,593)
Veterans, pensions, and post employment-related benefits	-	139	139
Advances from Others and Deferred Revenue	90	(4)	86
Other liabilities	(707)	(1,480)	(2,187)
Other Financing Sources:			
Imputed cost	(58,185)	-	(58,185)
Total Components of Net Cost That Are Not Part of Net Outlays	112,366	(198,038)	(85,672)
Components of Net Outlays That Are Not Part of Net Cost:			
Acquisition of Capital Assets	-	180,476	180,476
Financing Sources			
Transfers (in)/out without reimbursements	(120,193)	-	(120,193)
Total Components of Net Budgetary Outlays Not Part of Net Cost	(120,193)	180,476	60,283
Total Other Reconciling items	-	-	-
Total Net Outlays	$ (9,433,729)	$ 9,301,409	(132,320)
Agency Outlays, Net, Statement of Budgetary Resources			$ (132,319)
Unreconciled difference			$ (1)

Note 14. Disclosure Entities and Related Parties

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

Defense Information Systems Agency
Working Capital Fund
Required Supplementary Information
Fiscal Year 2025, Ending Sept. 30, 2025

Deferred Maintenance and Repairs Disclosures

In accordance with FASAB SFFAS 42 and FMR 6B, Chapter 12, 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 2025 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 is a lack of maintenance for software, it poses a security threat in the DISA environment. Based upon these overarching considerations, preventative maintenance takes place with current contracts to ensure operational and security capabilities. Since it is anticipated, due to the nature of the mission, the required maintenance is not deferred; therefore, not ranked or prioritized among other activities. In addition, as of FY 2025, all real property has been transferred out of the DISA WCF.

For FY 2025, 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, 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 assets 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.

Significant entities are required to: (1) describe their method for estimating deferred maintenance and repairs and how inflation in labor and materials costs is used to annually adjust the estimates and (2) report the minimum maintenance and repair amount needed to ensure that mission critical facilities remain mission capable. Maintenance and repairs are based on manufacturers' life cycle replacement criteria. Also building condition assessments are conducted to capture all systems, components, and sub-components. The assessments provide greater detail to forecast and budget for these repairs in the outyears. Funding is requested in the POM. There are limited funds even though forecasting has identified repair projects. An annual facility data call is issued to the organizations. Repair/Sustainment projects are prioritized: life safety, mission critical and repairs. Mission critical facilities have not been impacted by deferred maintenance. These facilities remain mission capable. Projects which are deferred to the following year – project costs have an escalation factor 2.1%. No significant changes in policy, identification, or treatment of DM&R have occurred since the last fiscal year.

Defense Information Systems Agency
Working Capital Fund
Other Information
Fiscal Year 2025, Ending Sept. 30, 2025

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

Figure 31- Summary of Financial Statement Audit

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

Figure 32- Summary of Management Assurances
Effectiveness of Internal Control over Financial Reporting (FMFIA§ 2)
Statement of Assurance: Unmodified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Fund Balance with Treasury	0	0	0	0	0	0
Accounts Payable/Expense	0	0	0	0	0	0
Accounts Receivable/Revenue	0	0	0	0	0	0
Internal Controls	0	0	0	0	0	0
Unmatched Transactions	0	0	0	0	0	0
Financial Reporting	0	0	0	0	0	0
Undelivered Orders	0	0	0	0	0	0
Unfilled Customer Orders	0	0	0	0	0	0
PPE	0	0	0	0	0	0
Total Material Weaknesses	0	0	0	0	0	0

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

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

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

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

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

Compliance Objective	Agency	Auditor
Federal Financial Management System Requirements	No lack of compliance noted	No lack of compliance noted
Applicable Federal Accounting Standards	No lack of compliance noted	No lack of compliance noted
USSGL at Transaction Level	No lack of compliance noted	No lack of compliance noted

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

23 October 2025

SUBJECT: Top Management and Performance Challenges Facing the Defense Information Systems Agency (DISA) in Fiscal Year 2026

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 2026.

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

The DISA OIG identified four 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 2026 include:

- Artificial Intelligence
- Human Capital
- Property Management and Accountability
- Increasing and Maintaining Readiness

RYAN.STEPHEN.MICHAEL.1300626706 Digitally signed by RYAN.STEPHEN.MICHAEL.1300626706 Date: 2025.10.23 11:39:53 -04'00'

Stephen M. Ryan
Inspector General

Challenge 1
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, and making predictions. Examples of AI enabled technology include chatbots that facilitate writing, tools for intelligence analysis, and autonomous targeting and weapon systems.

AI will transform warfare, and failure to adopt AI technology could hinder national security. According to the previous 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. In 2025, the White House published a national AI Action Plan that focuses on innovation, infrastructure, and international diplomacy and security.

While DISA is moving forward in the pursuit of integrating the use of AI into DISA's mission, the Agency faces a unique set of challenges. For example, AI requires significant computational power and storage, posing challenges for existing IT infrastructure and data management systems. Another challenge is integrating AI systems with existing legacy systems and infrastructure. Additionally, customizing generative AI models requires extensive datasets and DISA faces challenges in generating sufficient proprietary data to customize and train its AI tools. There is also an increased challenge of ensuring government-related materials, both Classified and Controlled Unclassified Information (such as Personal Identifiable Information (PII)) is protected from being uploaded into publicly available Generative AI tools. DISA also faces the risk of relying on a limited number of companies for AI services. Vendor lock-in could limit DISA's flexibility, stifle innovation by preventing exploration of alternative solutions and potentially create a single point of failure.

Challenge 2
Human Capital

Retaining and recruiting individuals with the right talent is critical and continues to be a top management challenge. Whether individuals are recent college graduates, high-performing industry professionals, or federal workers with years of experience in the field, DISA's challenge is to make the Agency a place sought out by high-caliber talent.

A significant challenge DISA faces is that the Agency competes for talent with the private sector. For example, DISA often struggles to compete with the private sector's higher salaries and more attractive compensation packages for highly skilled tech and cybersecurity professionals. Additionally, the need for specialized skills in areas like AI, machine learning, and advanced cybersecurity is growing at a faster pace than the government's ability to recruit and train new talent.

DISA's ability to retain and recruit faces additional pressures due to the recent changes in telework policies and the reduction in workforce. Since March of 2025, DISA employees have returned to the office fulltime; however, employees, especially those with in-demand skills, may prioritize work-life balance and flexible work arrangements, which may not always be readily available or perceived as available within the government sector. Additionally, DISA's reduction of its workforce by 10 percent through Deferred Resignation Program (DRP) and Voluntary Early Retirement Authority (VERA), coupled with a hiring freeze have introduced a set of unique challenges. Specifically, the DRP and VERA have incentivized the departure of experienced and tenured employees, including those in critical technical and leadership roles. This exodus risks a significant loss of institutional knowledge and expertise, impacting the agency's ability to maintain operations, respond to complex challenges, and mentor newer employees.

At the same time, DISA has expanded its mission requirements. For example, DISA has acquired IT service responsibilities for the Defense Advanced Research Projects Agency (DARPA), expanded Zero Trust architecture, accelerated secure cloud adoption, and adapted advanced AI tools. With fewer personnel, remaining employees may experience heavier workloads and increased pressure to maintain operations and deliver on mission-critical objectives. The added stress and workload can lead to burnout, decreased morale, and potentially contribute to further departures, creating a vicious cycle of attrition.

While acknowledging the challenges, the DISA Director said downsizing provides an opportunity to "ruthlessly realign and optimize" the agency to address its evolving mission. Specifically, DISA is also reorganizing its workforce, strategically refocusing on key priorities, and "surgically rehiring" to fill 210 critical gaps. DISA continues to strengthen the work culture, invest in key initiatives to attract and retain a talent pool skilled in critical thinking and diverse in ideas, backgrounds, and technical expertise. DISA is also forecasting needed skills through succession planning and improving how DISA markets career opportunities within the agency.

Challenge 3
Property Management and Accountability

Property management includes the functions of determining property requirements, receipt, storage, distribution, utilization, and disposal of property. DoD Instruction 5000.64 requires DoD components to maintain accurate property records for all government property acquired for $5,000 or more; government property furnished to a contractor; and as required by law, policy, regulation, or agency direction.

Property management and accountability is a challenge across DoD. The DoD IG identified material weaknesses in property management policies, procedures, and internal controls over inventory processes for DoD and its Components.

Property management and accountability is a top management challenge for DISA. For FY 2024, Property, Plant, and Equipment (PP&E) reported on DISA's balance sheets included General Fund (GF) amount of $509 million and Working Capital Fund (WCF) amount of $1.5 billion. In FY 2024, DISA's WCF Agency Financial Report (AFR) included a repeat significant deficiency pertaining to untimely asset activations and transfers between the GF and WCF. Similarly, the FY 2024 GF AFR reported a material weakness concerning timely activation of assets. Poor communication between program officials responsible for the assets and GF/WCF officials responsible for property accounting was cited as the cause for the lack of timeliness, resulting in material misstatements to PP&E as recorded on DISA's GF and WCF Balance Sheets.

The DISA OIG conducted several property audits and reported concerns relating to property management and accountability at DISA. Specifically, concerns included: property record accuracy, inventory management, organization and completeness of property loss reporting, proper oversight, property obsolescence, backlogs of property awaiting final disposal, and accountability of mobile devices. Furthermore, the DoD IG also found DISA did not maintain complete or accurate classified mobile device inventory records. These audit findings illustrate the challenges facing DISA when managing and accounting for property. The DISA OIG has made several recommendations to help improve the internal controls for property accountability.

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

Challenge 4
Increasing and Maintaining Readiness

DISA, as a Combat Support Agency (CSA), faces the ongoing challenge of maintaining a high level of readiness to deliver secure and reliable information technology and communications capabilities to the warfighter. This challenge requires strategic balancing between embracing technological modernization and ensuring robust operational capabilities, particularly in the light of evolving threats and dynamic operational environments. Failure in either domain can severely impact warfighter effectiveness and potentially jeopardize national security, highlighting the critical need for proactive management across key areas.

A critical component of DISA's readiness is its personnel. Addressing the skill gap caused by rapid technological advancements requires continuous learning and development programs focused on emerging technologies like cloud computing and cybersecurity. Ensuring certification alignment with operational needs and DoD directives is also paramount, alongside attracting and retaining top talent through a culture of innovation and competitive compensation. Fostering cross-functional expertise further enhances agility and collaboration, ensuring the workforce can effectively tackle complex challenges.

Operational exercises play a vital role in validating DISA's readiness and identifying areas for improvement. Exercises must accurately simulate real-world scenarios and encompass end-to- end system functionality, requiring sufficient resource allocation and data-driven analysis. Exercising seamless communication and information sharing between mission partners and allies is crucial during crises. By implementing a comprehensive exercise program that integrates lessons learned, DISA can continuously refine its capabilities and enhance its responsiveness.

Finally, a robust Continuity of Operations (COOP) plan is essential for maintaining critical services during disruptions. This demands regular plan validation through exercises, ensuring redundancy and resilience in infrastructure and personnel, and integrating cybersecurity considerations into COOP strategies. Effective communication and coordination across DISA and with external stakeholders during emergencies are also paramount. By prioritizing these areas, DISA can ensure it can maintain essential services and support the warfighter, even in the face of significant disruptions.

OFFICE OF THE INSPECTOR GENERAL

The Office of the Inspector General (OIG) is an impartial factfinder 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 provide 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 ensuring external agency objectives are met while minimizing the impact to DISA operations. OIG Liaison supports DISA as a whole by providing:

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

Payment Integrity

For compliance with the Payment Integrity Information Act of 2019 (Pub. L. No. 116-117, 31 U.S.C. § 3352 and § 3357), DISA has an internal control structure in place to mitigate improper payments that could result in payment recovery actions. Actions taken to prevent overpayments include testing and review of civilian time and attendance, travel payments, and purchase card transactions. Controls are in place through established policy and procedures; training; separation of duties; and data mining to identify risks and fraud vulnerabilities. Additionally, the DFAS, as DISA's accounting service provider, performs overpayment recapture functions on behalf of DISA. The DFAS includes DISA transactions in their sampling populations for improper payment testing for civilian payroll and travel. In FY 2025, improper payments have been detected; however, the majority of those identified have an immaterial or no financial impact (attributable to timing of authorization and supporting documentation). A CAP has been implemented to mitigate future inconsistencies. DISA provides information that is consolidated into the Annual OMB Program and Agency Surveys and OMB uses that data to populate the PaymentAccuracy.gov website.

Federal Entity Trading Partner Information

DISA's intragovernmental balance reconciliation process begins with extracting and validating trading partner data from FAMIS, encompassing accounts receivable (AR), revenue, accounts payable (AP), and expense transactions. This validated data, representing either the buyer or seller side, is shared with the trading partner, who reciprocates with their corresponding data. A detailed reconciliation is then performed to identify variances, which are subsequently analyzed to determine their drivers. Resolution involves adjusting DISA's records via Journal Vouchers in DDRS when the trading partner provides supporting documentation or requesting the trading partner to adjust their records to match DISA's when the DISA's data is better supported. All reconciliation activities, variance analyses, and adjustments are meticulously documented to maintain a complete audit trail for auditability and compliance.

DISA GF is DISA WCF's largest trading partner by volume, followed by Army GF, AF GF, Navy GF, DFAS, GSA, and FAA. DISA WCF also collaborates directly with DeCA, USACE, USMC GF, DTRA, DHRA, DCAA, Army WCF, DARPA, TJS, and MDA on reconciliations and adjustments, and while the transaction volume with these partners is lower, direct collaboration is crucial to ensure balance alignment.

To comply with the TFM deadline and enable G-Invoicing usage for all Buy/Sell transactions by Fall 2025, the implementation schedule includes an upgrade of FAMIS to Oracle ERP 12.2.14 and implementing DISA intradepartmental orders, targeting completion around mid-October 2025, while acknowledging potential impediments such as timeline dependencies, GTC modification limitations, lack of an Oracle solution for seller-initiated modifications, and general buyer-seller disputes.

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

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

November 7, 2025

MEMORANDUM FOR UNDER SECRETARY OF WAR (COMPTROLLER)/
CHIEF FINANCIAL OFFICER, DoW
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 2025
(Project No. D2025-D000FL-0055.000, Report No. DODIG-2026-009

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 year ended September 30, 2025. The contract required Kearney to provide a report on internal control over financial reporting and compliance with provisions of applicable laws and regulations, contracts, and grant agreements, and to report on whether the DISA Working Capital Fund's financial management systems substantially complied with the requirements of the Federal Financial Management Improvement Act of 1996. The contract required Kearney to conduct the audit in accordance with generally accepted government auditing standards (GAGAS); Office of Management and Budget audit guidance; and the Government Accountability Office/Council of the Inspectors General on Integrity and Efficiency, "Financial Audit Manual," Volume 1, June 2025, Volume 2, June 2024, and Volume 3, August 2025. 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 year ended September 30, 2025, were presented fairly, in all material respects, and in accordance with Generally Accepted Accounting Principles.

Kearney's separate report, "Independent Auditor's Report on Internal Control Over Financial Reporting," did not identify any material weaknesses related to the DISA Working Capital Fund's internal controls over financial reporting. *

Kearney's additional report, "Independent Auditor's Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements," did not identify any instances of noncompliance with provisions of laws and regulations, contracts, and grant agreements.

In connection with the contract, we reviewed Kearney's reports and related documentation and discussed them with Kearney's representatives. Our review, as differentiated from an audit of the financial statements and related notes in accordance with GAGAS, was not intended to enable us to express, and we do not express, an opinion on the DISA Working Capital Fund FY 2025 Financial Statements and related notes. Furthermore, we do not express conclusions on the effectiveness of internal controls over financial reporting, on whether the DISA Working Capital Fund's financial systems substantially complied with Federal Financial Management Improvement Act of 1996 requirements, or on compliance with provisions of applicable laws and regulations, contracts, and grant agreements. Our review disclosed no instances in which Kearney did not comply, in all material respects, with GAGAS. Kearney is responsible for the attached November 7, 2025 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.

Lorin T. Venable

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

Attachments: As stated

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

Independent Auditor's Report

KEARNEY& COMPANY

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

INDEPENDENT AUDITOR'S REPORT

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

Report on the Audit of the Financial Statements

Opinion

We have audited the financial statements of the Defense Information Systems Agency (DISA) Working Capital Fund (WCF), which comprise the Balance Sheet as of September 30, 2025, the related Statements of Net Cost and Changes in Net Position, and the combined Statement of Budgetary Resources (hereinafter referred to as the "financial statements") for the year 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, 2025 and its net cost of operations, changes in net position, and budgetary resources for the year then ended in accordance with accounting principles generally accepted in the United States of America.

Basis for Opinion

We conducted our audit in accordance with auditing standards generally accepted in the United States of America (GAAS); the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 24-02, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards are further described in the ***Auditor's Responsibilities for the Audit of the Financial Statements*** section of our report. We are required to be independent of DISA WCF and to meet our other ethical responsibilities in accordance with the relevant ethical requirements relating to our audit. 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 GAAS and Government Auditing Standards will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

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

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

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

Required Supplementary Information

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

Other Information

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

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

Other Reporting Required by *Government Auditing Standards*

In accordance with *Government Auditing Standards* and OMB Bulletin No. 24-02, we have also issued reports, dated November 7, 2025, on our consideration of DISA WCF's internal control over financial reporting and on our tests of DISA WCF's compliance with certain provisions of laws, regulations, contracts, and grant agreements, as well as other matters. The purpose of those reports is solely 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 the effectiveness of DISA WCF's internal control over financial reporting or on compliance and other matters. Those reports are an integral part of an audit performed in accordance with *Government*

Auditing Standards and OMB Bulletin No. 24-02 in considering DISA WCF's internal control over financial reporting and compliance.

Alexandria, Virginia
November 7, 2025

KEARNEY& COMPANY

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

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

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

We have audited, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 24-02, *Audit Requirements for Federal Financial Statements*, the financial statements, and the related notes to the financial statements of the Defense Information Systems Agency (DISA) Working Capital Fund (WCF) as of and for the year ended September 30, 2025, which collectively comprise DISA WCF's financial statements, and we have issued our report thereon dated November 7, 2025.

Report on Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered DISA WCF's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of DISA WCF's internal control. Accordingly, we do not express an opinion on the effectiveness of DISA WCF's internal control. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 24-02. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies; therefore, material weaknesses or significant deficiencies may exist that have not been identified. Given these limitations, during our audit,

KEARNEY& COMPANY

we did not identify any deficiencies in internal control that we consider to be material weaknesses.

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

During the audit, we noted certain additional matters involving internal control over financial reporting that were reported to DISA WCF's management throughout the audit.

The Defense Information Systems Agency Working Capital Fund's Response to Findings

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

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and the results of that testing, and not to provide an opinion on the effectiveness of DISA WCF's internal control. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 24-02 in considering DISA WCF's internal control. Accordingly, this report is not suitable for any other purpose.

Alexandria, Virginia
November 7, 2025

KEARNEY& COMPANY

Schedule of Findings

Significant Deficiencies

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

Exhibit 1: Significant Deficiencies and Sub-Categories

Significant Deficiency	Significant Deficiency Sub-Categories
I. Fund Balance with Treasury	A. Statement of Differences Reconciliation and Reporting Processes B. Suspense Reconciliation and Reporting Processes
II. Property, Plant, and Equipment	A. Untimely Asset Activation B. Foreign Currency Issue on Leases
III. Information Technology	A. Defense Information Systems Agency Risk Management Framework B. Financial Accounting Management Information System Database Audit Logging and Monitoring C. Complementary User Entity Controls Implementation D. Cross-System Segregation of Duties E. Budget Execution Reporting Tool Contingency Plan Testing

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

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

A. Statement of Differences Reconciliation and Reporting Processes
B. Suspense Reconciliation and Reporting Processes

A. Statement of Differences Reconciliation and Reporting Processes

Background: DISA WCF's service organization provides daily Non-Treasury Disbursing Office (NTDO) disbursing services under various Agency Location Codes (ALC), often referred to as Disbursing Station Symbol Numbers (DSSN). Additionally, DISA WCF's service organization provides monthly Department of the Treasury (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, Check Issued, and G-Invoicing differences monthly. DISA WCF's service organization has three reporting ALCs responsible for month-end reporting of collections and disbursements to Treasury. Further, as a reporting entity, DISA WCF is responsible for researching and resolving differences identified on the FMS 6652 for the ALCs that process its transactions to determine whether its transactions are included in an SOD and erroneously omitted from its financial statements.

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

Condition: DISA WCF, in coordination with its service organization, has not implemented a monitoring control to ensure that transactions that compose the SOD balances in DISA WCF's primary DSSNs do not contain DISA WCF collections and disbursements that should be recognized in DISA WCF's 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 WCF's service organization prepares quarterly SOD materiality assessments at the DSSN level, for DISA WCF's service organization-managed DSSNs, to identify the total count and dollar value of the SOD transactions resolved to DISA WCF and other Defense agencies, the uncleared SOD transactions included in the assessments are significant.

Cause: DISA WCF's service organization's process to create the Universe of Transactions (UoT) for SODs is a time-intensive and manual process that requires the consolidation of multiple files from various sources. The SOD UoTs continue to contain a high volume of collections and disbursements which require manual research and resolution. That manual research and resolution supports the production of the final UoTs and materiality assessments but takes a significant amount of time, resulting in them being 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 "to be determined" (TBD).

While DISA WCF's service organization has continued efforts to identify root causes by DSSN to reduce SOD balances and clear transactions to Department of War (DOW) entities timely, shared ALCs and lack of Line of Accounting (LOA) information continue to make it difficult to resolve differences timely.

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

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

1. Pursuant to receiving the necessary information and documentation from DISA WCF's service organization, develop and implement procedures to identify DISA WCF's actual or estimated SOD balances for recording and reporting adjustments within the financial statements.
2. Assist its service organization by providing supporting information to clear transactions reported in SODs timely.
3. Work with Treasury, the Office of the Secretary of War, DISA WCF's service organization, and other parties to continue transitioning away from using monthly NTDO reporting ALCs to daily TDO reporting ALCs.
4. Consider any limitations to its service organization's SOD process and develop compensating controls to reconcile SOD balances to minimize the risk of a potential material misstatement.
5. Coordinate with its service organization to monitor and track the resolution of SODs cleared to DISA WCF to enable DISA WCF to perform root cause analysis and develop compensating controls for financial reporting purposes.
6. Coordinate with its service organization to continue to develop procedures to determine what portion of the SOD balances, if any, should be attributed to DISA WCF for financial reporting in a timely manner and made available for year-end financial reporting purposes.
7. Coordinate with its service organization to continue to monitor and track the resolution of SOD activity cleared to DISA WCF to enable the entity to perform root cause analysis. This includes further research and resolution over the transactions not resolved in the UoTs and listed as "TBD."
8. Coordinate with its service organization to assess and identify ALCs that primarily report collection and disbursement activity to Treasury on behalf of DISA WCF.
9. Coordinate with its service organization to coordinate recurring meetings with DISA WCF to help resolve outstanding differences.

KEARNEY& COMPANY

B. Suspense Reconciliation and Reporting Processes

Background: DISA WCF's service organization and the Office of the Under Secretary of War (Comptroller) (OUSW[C]) Enterprise Financial Transformation (EFT) manage, report, and account for FBWT budget clearing (suspense) account activities to Treasury. In addition to monitoring and approving the FBWT reconciliations performed by its service organization and OUSW(C) on its behalf, DISA WCF is responsible for the complete and accurate reporting of FBWT on its financial statements and disclosures.

Suspense accounts temporarily hold unidentifiable general, revolving, special, or trust fund collections or disbursements that belong to the Federal Government. An "F" preceding the last four digits of the fund account symbol identifies these funds. These accounts are to be used only when there is a reasonable basis or evidence that the collections or disbursements belong to the U.S. Government and, therefore, properly affect the budgetary resources of the DOW activity. None of the collections recorded in suspense accounts are available for obligation or expenditure while in suspense. Agencies should have a process to research and properly record suspense account transactions in their general ledgers (GL) timely. Transactions recorded in DOW suspense are required to be reconciled monthly and moved to the appropriate LOA within 60 business days from the date of transaction.

On behalf of DOW agencies, including DISA WCF, DISA WCF's service organization prepares materiality assessments quarterly using a combination of historical data and the current quarter's raw UoTs to estimate the potential impact of outstanding suspense transactions to each DOW entity. The raw UoTs have not been fully researched to identify transaction count and dollar amount impact to DISA WCF and other DOW entities and could contain summary lines. Fully researched UoTs are not available until 55 days after quarter-end and year-end financial reporting timelines.

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

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

Condition: DISA WCF, in coordination with its service organization, has not implemented sufficient internal control activities to ensure that transactions recorded in suspense accounts do not contain DISA WCF collections and disbursements that should be recognized in the DISA WCF accounting records. Additionally, DISA WCF does not have effective controls over the validation of its recorded disbursements and collections, as they impact complementary line items, including AP, AR, and related line items on the Statement of Budgetary Resources, to ensure it is accounting for all transactions that should be reported on their books. 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 WCF's service organization prepares quarterly suspense materiality assessments for each Treasury Index (TI) to advise DISA WCF and other Defense agencies of the potential count and dollar amount of suspense transactions belonging to them, based on previously resolved and cleared suspense transactions, the uncleared suspense transactions included in the assessment are material.

Cause: DISA WCF's suspense activity is not recorded in unique suspense accounts, but rather in shared TI-97, TI-57, TI-21, and TI-17 suspense accounts. DOW suspense accounts continue to contain a high volume of collections and disbursements which require manual research and resolution. That manual research and resolution is what supports the production of the final UoTs and materiality assessments, but takes a significant amount of time, which is the cause of them not being available in a timely manner for financial reporting. Additionally, at the time of UoT availability, there has been a significant volume of transactions for a material dollar amount in suspense that has not been identified to an entity and is listed in the UoT as "TBD," as well as unknown samples that require on-site testing and summary line transactions.

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

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

Recommendations: Kearney recommends that DISA WCF perform the following:

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

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

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

A. Untimely Asset Activation
B. Foreign Currency Issue on Leases

Background for Items II.A and II.B: The March 31, 2025 DISA WCF General Property, Plant, and Equipment (PP&E) was composed of equipment, software, Construction-in-Progress (CIP),

and Right-to-Use Lease assets with a net book value of $1.5 billion. DISA WCF utilizes the Enterprise Logistics Management System (ELMS), formally known as the Defense Property Accountability System (DPAS), as its property management system, which provides property financial reporting information. DISA WCF utilizes a separate lease repository system, FedLease, for storing, analyzing, and reporting lease accounting information.

In FY 2024, DISA WCF implemented changes regarding Right-To-Use Leases from the SFFAS No. 54, *Leases*. The Right-To-Use Leases account records the right to control an asset during the lease term in leases other than short-term, intragovernmental, and lease contracts that transfer ownership. The account is measured as the total amount of initial lease liability at the beginning of the lease term, lease payments made at or before the start of the lease term, and any indirect lease costs necessary to put the asset into service per the TFM. DISA WCF identifies telecommunication (Communication Service Authorization [CSA]) and non-telecommunication leases in accordance with SFFAS No. 54. New leases are identified monthly, and these new leases undergo the process of abstraction, in which the information needed for the Right-To-Use Lease recording is pulled from the Integrated Defense Enterprise Acquisition System (IDEAS). After the new leases have been abstracted, the data is uploaded to FedLease.

DISA WCF determines which CSAs are active by identifying which have a monthly recurring charge (MRC) based on the E-Trans Report. The current-month active CSA leases and prior-month active CSA leases are compared to identify new additions and early disconnections. For additions, DISA WCF utilizes the IDEAS Contract Line Item Number (CLIN) System Data Report needed for lease data abstraction. DISA WCF performs lease data abstraction for all monthly CSA lease additions and runs the abstraction tool to extract data fields into the FedLease upload template using the CLIN System Data Report. It is the responsibility of DISA WCF management to ensure that Right-To-Use Leases are recorded timely in the financial system.

DISA WCF must record capital assets accurately in the correct accounting period. Leases are to be recorded at the commencement of the lease term per SFFAS No. 54. Additionally, DISA WCF must translate foreign currency transactions to U.S. dollar equivalents per TFM, Volume I, Part 2, Chapter 3200, *Foreign Currency Accounting And Reporting,* Section 3235.10.

A. Untimely Asset Activation

Condition: Substantive audit testing of DISA WCF's Right-To-Use Lease additions identified untimely Right-To-Use Lease activations. Specifically, testing identified 20 Right-To-Use Leases with an activation date in FY 2024. As a result, DISA WCF performed an analysis over the Right-To-Use Lease population and identified 131 Right-To-Use Lease with an activation date from FY 2024 that understated the population by $23.4 million as of September 30, 2024.

Cause: The untimely Right-To-Use Lease activations resulted from inconsistent or ineffective communication between vendors or mission partners responsible for the Right-To-Use Leases and the DISA WCF officials who are responsible for property accounting, due to the volume and complexity of Right-To-Use Leases.

Effect: DISA WCF understated the Right-To-Use Lease balance by $23.4 million on the September 30, 2024 WCF financial statements. 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 WCF perform the following:

1. Increase communication with mission partners to monitor Right-To-Use Lease activations and ensure the Right-To-Use Leases are recorded in the financial statements in a timely manner.
2. Implement an effective control and process to notify DISA WCF management of Right-To-Use Lease activations, in addition to enhanced coordination with vendors and mission partners on Right-To-Use Lease activations.

B. Foreign Currency Issue on Leases

Condition: Substantive audit testing of DISA WCF's Right-To-Use Lease additions and disposals identified discrepancies between the total obligation balances and the Right-To-Use Lease balances in FedLease. Specifically, testing identified 17 Right-To-Use Leases denominated in a foreign currency, which was not converted to United States Dollars (USD). As a result, DISA WCF performed an analysis over the entire Right-To-Use Lease population and identified 145 Right-To-Use Leases recorded in a foreign currency, but not converted to USD, and identified that the population was overstated by $38 million as of September 30, 2024.

Cause: DISA WCF utilized the IDEAS CLIN Data Report to identify new leases for input into FedLease. The report did not contain a data field to designate translated USD values for the new leases stated in foreign currencies input into FedLease, which resulted in discrepancies between the total obligation balances in IDEAS and the Right-To-Use Lease costs.

Effect: DISA WCF overstated the Right-To-Use Lease and lease unfunded liability balances by $38 million and $31 million, respectively, on the September 30, 2024 WCF Balance Sheet. The lack of an effectively designed control to identify and convert lease terms in foreign currencies increases the risk that misstatements will continue to occur and not be prevented, or detected and corrected, in a timely manner.

Recommendations: Kearney recommends that DISA WCF perform the following:

1. Identify data fields to capture and report foreign currency leases at their translated USD values using the exchange rates within IDEAS.
2. Update control and process refinements to ensure foreign currency leases are denominated in translated USD amounts and not reported at their original currency

values. This may include a fluctuation analysis to adjust for foreign currencies that have significant volatility.

III. Information Technology (*Modified Repeat Condition)*

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

A. Defense Information Systems Agency Risk Management Framework
B. Financial Accounting Management Information System Database Audit Logging and Monitoring
C. Complementary User Entity Controls Implementation
D. Cross-System Segregation of Duties
E. Budget Execution Reporting Tool Contingency Plan Testing

A. Defense Information Systems Agency Risk Management Framework

Background: DISA WCF meets the DOW's information technology (IT) needs through enterprise security architectures, smart computing options, and other leading-edge IT opportunities. Specifically, DISA WCF delivers hundreds of IT support services capabilities and has the capacity to host, support, engineer, test, or acquire IT services.

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

DISA WCF utilizes Enterprise Mission Assurance Support (eMASS) to implement the RMF to its respective systems. eMASS is a web-based Government Off-the-Shelf solution that automates a broad range of services for comprehensive, fully integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of RMF for DOW IT Package Reports.

NIST published SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, in September 2020 and SP 800-53A, Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, in January 2022. Per Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, organizations have a one-year grace period prior to finalizing their implementation of any updated requirements.

On September 16, 2024, the DISA Authorizing Official (AO) issued a memorandum announcing DISA's transition to NIST SP 800-53, Rev. 5. The memorandum states:

> "DISA, Enterprise Integration and Innovation, Risk Management Directorate (RE), recognizes the migration of DISA's System inventory from NIST SP 800-53 Revision 4 to Revision 5 (hereafter Rev. 4 and Rev. 5) is a significant undertaking. With due diligence, the Assessment and Authorization (RE5) staff have prepared a detailed Transition Plan to prepare for DISA's implementation with the goal of ensuring internal and external partners are well informed and provided the necessary knowledge leading to a smooth transition and successful outcome."

Condition: DISA did not update its RMF documentation, processes, procedures, and System Security Plans (SSP) for most of its internal systems to reflect updated requirements presented within NIST SP 800-53, Rev. 5 in the prescribed timeline set forth by OMB Circular A-130, Appendix I. While there is a mention of Rev. 5 in the FABS SSP, the system has not yet been authorized under the new Rev. 5 controls.

Cause: While the DISA AO released a NIST SP 800-53, Rev. 5 transition memorandum, dated September 16, 2024, outlining a plan to implement the Rev. 5 control baseline, the new control set and baseline did not become available in eMASS to DISA system owners until March 2025. In March 2025, DISA WCF personnel began to implement and validate NIST SP 800-53, Rev. 5 controls within the Budget Execution Reporting Tool (BERT), Financial Accounting Management Information System (FAMIS), and Financial Accounting and Budgeting System (FABS) system environments, but, due to time constraints, each system will not be authorized under Rev. 5 until their current authorization expires.

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

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Update the system-specific RMF documentation, processes, procedures, SSPs, and appropriate security documentation upon reauthorization set forth by the NIST SP

800-53, Rev. 5 security controls implementation. DISA WCF should continue to implement and validate the Rev. 5 controls for the BERT, FAMIS, and FABS systems and re-authorize each system under Rev. 5 on or before expiration of the current Authorization to Operate (ATO).

B. Financial Accounting Management Information System Database Audit Logging and Monitoring

Background: The DISA WCF Accounting Integration Branch (CFA33) is responsible for IS security management and audit logging and monitoring for FAMIS.

As a turn-key financial management system software solution, FAMIS is based on Oracle eBusiness Suite (EBS) R12.2.9 to support the following application family of products: GL, AR, AP, Federal Administration, Project Costing, Project Billing, Project Contracts, Purchasing, and Procurement. The resulting system implements Oracle Identity and Access Management to interface with EBS to provide Common Access Card authentication to EBS.

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

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

DISA WCF should review and analyze system audit records per NIST SP 800-53, Rev. 5, Control AU-6, "Audit Record Review, Analysis, And Reporting."

Condition: While DISA WCF implemented a process to log and review configuration changes to the FAMIS database daily, DISA WCF personnel did not adhere to the required review timeframe of seven days following the daily e-mail-generated audit log reports. Specifically, DISA WCF personnel did not perform timely reviews for one of the 37 (~3%) FAMIS database audit logs sampled for testing.

Cause: Agency personnel implemented a process to log all configuration changes to the FAMIS database; however, DISA WCF failed to consistently perform timely reviews over the database audit logs, as one of the 37 sampled reviews (~3%) was not reviewed within the seven-

day timeframe, as defined within the FAMIS SSP. DISA WCF personnel inadvertently missed the sample during the General Fund (GF) migration from Defense Agencies Initiative (DAI) to FAMIS.

Effect: Failure to review FAMIS database audit logs in a timely manner may result in DISA WCF personnel being unaware of potential issues that could affect the FAMIS database. Those issues may affect the integrity and availability of the FAMIS database, as well as the security baseline. Untimely audit log reviews may result in inappropriate or malicious actions remaining undetected for an extended period, which may hinder DISA WCF's ability to initiate prompt corrective action.

Recommendations: Kearney recommends that DISA WCF perform the following:

1. Consistently perform reviews over the database audit logs in a timely manner, as defined within FAMIS policies, as well as Federal and/or DOW criteria (i.e., seven days).
2. Develop and implement a quality control (QC) process over the FAMIS database logging and monitoring review process. The QC process should include procedures to ensure FAMIS database logs are generated and reviewed within prescribed timelines.
3. Continue to retain evidence of the review of FAMIS database logs for third-party review.

Background for Items III.C and III.D: DISA WCF utilizes several service organizations to support its operations and mission. As such, DISA WCF obtains assurances from each organization regarding the effectiveness of the organization's internal controls related to the service(s) provided. Specifically, each organization provides a written assertion that accompanies a description of its service(s) and related IS(s). These assertions are communicated via a System and Organization Controls (SOC) report. In FY 2025, each service organization provided DISA management with a SOC 1®, Type 2 report, *Report on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, to report on the design and operating effectiveness of its internal controls.

In many cases, service organizations design their controls in support of their service(s) with the assumption that the user entities (i.e., customers or users of the service[s]) will implement certain controls (i.e., Complementary User Entity Controls [CUEC]) to achieve the overall control objectives and create a secure computing environment. Specifically, Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification*, defines CUECs as controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the service organization's system. DISA WCF is responsible for ensuring that CUECs are properly implemented and operating effectively in order to rely on the results of the SOC 1® reports.

DISA WCF relies on multiple service organizations and their respective SOC reports to gain an understanding of the security posture of each of the systems upon which DISA relies. For example, DISA WCF utilizes the Defense Logistics Agency's (DLA) DAI system for time and attendance; DLA's ELMS for logistics and property management services; DLA's Wide Area Workflow (WAWF) for management of goods and services; the Defense Finance and Accounting Service's (DFAS) Defense Cash Accountability System (DCAS) for transaction distribution services; DFAS's Defense Civilian Pay System (DCPS) for Federal civilian payroll services; DFAS's Defense Departmental Reporting System (DDRS) for financial reporting services; DFAS's Automated Disbursing System (ADS) for standard disbursing services; the Defense Manpower Data Center's (DMDC) Defense Civilian Personnel Data System (DCPDS) for processing payroll affecting civilian human resource transactions; the DoD Office of the Chief Digital and Artificial Intelligence Officer (OCDAO) Directorate of Scaled Capabilities Advancing Analytics (Advana) to support budgetary processes; and DFAS's Mechanization of Contract Administration Services (MOCAS) for managing procurement payment and entitlement determinations of contract data for delivery and other reporting.

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

Additionally, DISA WCF should identify, document, and implement segregation of duties (SD) controls per NIST SP 800-53, Rev. 5, Control AC-5, "Separation of Duties."

C. Complementary User Entity Controls Implementation

Condition: DISA has not effectively implemented all CUECs required by its service organizations. Based on a subset of high-risk CUECs (e.g., periodic access reviews and removals) required by DISA WCF's service organizations, examples of control deficiencies which indicate that CUECs are not operating effectively include the following:

- DISA WCF did not consistently remove users' access as part of the periodic access review for the DAI application
- DISA WCF did not consistently remove or disable access for DISA WCF users of the Advana application upon separation from the agency.

Cause: Although DISA WCF was aware of the requirements for implementing the CUECs and had begun implementation, it had not finalized implementation of all CUECs as of the end of the FY 2025 financial statement audit. Per the CUEC workbook, DISA WCF documented the CUECs that are scheduled for design and implementation testing during DISA WCF's three-year CUEC test cycle. Specifically, DISA WCF continues to identify and implement compensating controls to remediate control gaps noted during the reviews performed over the CUECs identified within each service organization's SOC 1®, Type 2 report. Additionally, DISA WCF maps the relevant CUECs to the corresponding DISA WCF-performed control. Further, due to

the large number of CUECs, DISA WCF established a phased approach and executed it to test CUECs based on level of risk and document results of implementation.

Effect: DISA WCF's failure to effectively implement internal controls to address all required CUECs may result in ineffective controls and the inability to rely on the SOC 1®, Type 2 reports. 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) increase the risk of a negative impact to the confidentiality, integrity, and availability of data supporting DISA WCF's financial statements.

Recommendations: Kearney recommends that DISA WCF perform the following:

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

D. Cross-System Segregation of Duties

Condition: DISA WCF has not clearly defined the SD conflicts that may exist between all the systems it utilizes for its day-to-day operation in supporting its financial statements, including those managed by external service organizations. Specifically, DISA WCF has not clearly defined the potential conflicts that may arise when individuals have access to multiple systems, including external service organization systems.

Cause: Although DISA WCF was aware of the requirements for implementing the CUECs and had begun implementation, it had not finalized implementation of all CUECs as of FY 2025. DISA WCF has continued to refine its existing process, as documented within the CUEC Review Process narrative. Specifically, DISA WCF continues to identify and implement compensating controls to remediate control gaps identified during the reviews performed over the CUECs noted within each service organization's SOC 1®, Type 2 report. Additionally, DISA WCF maps the relevant CUECs to the corresponding DISA WCF-performed control. Further, due to the large number of CUECs, DISA WCF established a phased approach and executed it to test CUECs based on level of risk and document results of implementation.

Effect: DISA WCF's failure to develop/implement an effective process to document and monitor potential SD conflicts across service organizations results in increased risk that a user may possess unauthorized and/or unmonitored conflicting roles. Users with access privileges that create SD conflicts may perform functions that impact the integrity of the data within the system and increase the risk of fraudulent activity.

Recommendations: Kearney recommends that DISA WCF perform the following:

1. Develop and document a comprehensive access control framework that identifies incompatible duties across all systems, including those managed by third-party service organizations.
2. Implement regular reviews of user access rights to detect and remediate conflicts, ensuring roles are appropriately segregated and aligned with internal control requirements.
3. Establish a centralized governance process to oversee access provisioning, including coordination with service organizations to ensure consistent enforcement of SD controls across all environments.

E. Budget Execution Reporting Tool Contingency Plan Testing

Background: BERT is an online management IS used by DISA WCF, DISA Chief Financial Executive, and CFA33, along with others, to provide a Management Information Tool to supplement FAMIS-WCF (Enterprise Information Services' [EIS] accounting system and sole source of official accounting data). Utilizing Commercial-Off-the-Shelf software and a SQL database, BERT is installed on multiple DISA-accredited devices residing on the Datacenter Montgomery environment located in Montgomery, AL.

It is the intent of the Continuity of Operations (COOP) Plan to assure that the BERT application is minimally disrupted in the event of disaster (i.e., accidental, natural, or man-made), compromise of the system, or failure. The COOP Plan applies to the BERT Application Support Team and end users of the application. In the event of a disastrous event, recovery of the application and mission-essential functions, as well as essential business functions, will be a joint effort between the BERT Application Support Team and remote management site. Although most disasters cannot be predicted, the BERT Application Support Team possesses responsibilities that must be executed before, during, and after a disastrous event. Familiarity with the COOP Plan, assigned responsibilities, and situational awareness will help to prevent loss of data, minimize damages, and reduce or mitigate disruptions in operations.

According to NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, contingency planning for ISs involves a coordinated strategy, including plans, procedures, and technical measures, that will allow and aid in the recovery of data and operations within ISs following a disruption. Contingency planning usually includes at least one of the following approaches to restore disrupted services: restoring ISs using alternate equipment; performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions); recovering IS operations at an alternate location (typically acceptable for only long-term disruptions or those physically impacting the facility); and implementation of appropriate contingency planning controls based on the IS's security impact level.

DISA WCF should perform contingency plan tests over its systems and applications per NIST SP 800-53, Rev. 5, Control CP-4, "Contingency Plan Testing."

Condition: DISA WCF was unable to complete its annual test of the contingency plan over the BERT application during FY 2025.

Cause: At the end of FY 2024, DISA received a letter from the DISA J9 Hosting and Compute, stating that support for a shared COOP will end effective September 30, 2024. Upon receipt of this letter, DISA WCF personnel began the process of transitioning to a dedicated COOP method of testing its contingency plan. During the course of FY 2025, DISA WCF personnel made significant efforts to fulfill this transition; the team attended meetings, requested additional funding, and completed a baseline change request to begin the process. However, due to time constraints, the BERT Team was unable to complete the transition to a dedicated COOP in FY 2025.

Effect: Failure to perform testing on the contingency plan for BERT on a consistent and annual basis may result in DISA WCF's inability to reliably recover the application in the event of disaster. If BERT cannot be recovered after a disaster, DISA WCF's operations may be affected due to lack of availability of system functionality and data for users of the system.

Recommendation: Kearney recommends that DISA WCF perform the following:

1. Immediately upon implementation of the dedicated COOP, perform a contingency plan test for the BERT application, then document the results and any issues encountered during execution and testing of the plan.

* * * * *

KEARNEY&
COMPANY

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

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

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

We have audited, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 24-02, *Audit Requirements for Federal Financial Statements*, the financial statements, and the related notes to the financial statements of the Defense Information Systems Agency (DISA) Working Capital Fund (WCF) as of and for the year ended September 30, 2025, which collectively comprise DISA WCF's financial statements, and we have issued our report thereon dated November 7, 2025.

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether DISA WCF's financial statements are free from material misstatement, we performed tests of DISA WCF's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of the financial statement amounts and disclosures, including the provisions referred to in Section 803(a) of the Federal Financial Management Improvement Act of 1996 (FFMIA). However, providing an opinion on compliance with those provisions was not an objective of our audit; accordingly, we do not express such an opinion. The results of our tests, exclusive of those referred to in FFMIA, disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 24-02.

The results of our tests of compliance with FFMIA disclosed no instances in which DISA WCF's financial management systems did not comply substantially with Section 803(a) requirements related to Federal financial management system requirements, applicable Federal accounting standards, or application of the United States Standard General Ledger at the transaction level.

KEARNEY& COMPANY

Purpose of this Report

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

Alexandria, Virginia
November 7, 2025

DISA Management Comments to Auditor's Report

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

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

Mr. Gorrell:

DISA acknowledges receipt of Kearney & Company's final audit report for DISA's FY 2025 Working Capital Fund (WCF) financial statements.

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

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

SPONSELLER.JUSTIN.C.1258339246
Digitally signed by SPONSELLER.JUSTIN.C.1258339246
Date: 2025.11.07 16:04:35 -05'00'

JUSTIN SPONSELLER
Chief, Accounting and
Audit Operations

Appendix A- DISA Organizational Chart

DCDC

DISA Director, DCDC Commander

- **Senior Enlisted Leader**
- **Deputy Director**
- **Chief of Staff**
- **J1 – Manpower & Personnel Directorate**
- **J2 – Intelligence Directorate**
- **J3/5/7 – Operations, Plans & Exercises Directorate**
- **J4 – Facilities & Logistics Directorate**
- **J6 – Command, Control, Communications, and Computers Enterprise Directorate**
- **J8 – Office of the Chief Financial Officer**
- **J9 – Hosting & Compute Directorate**
- **Acquisition Directorate**
  - Component Acquisition Executive
  - Cyber Program Executive Office
  - Transport Program Executive Office
  - Service Program
- **Enterprise Integration and Innovation Directorate**
  - Emerging Technology Directorate
  - Enterprise Engineering Directorate
  - Risk Management Directorate
  - Office of the Chief Information Officer
  - Office of the Chief Data Officer
  - Joint Interoperability Test Command
- **Special Staff**
  - Chaplain Program Management Office
  - Public Affairs
  - General Counsel
  - Inspector General
  - Office of Small Business Programs
  - Protocol
  - Office of Equal Employment Opportunity Compliance
- **ADCON Organizations**
  - Secretary of Defense Communications
  - White House Communications Agency
  - White House Situation Support Staff
- **Procurement Services Directorate**
  - Defense Capabilities Contracting Division
  - Business Operations Division
  - Contract Policy & Contract Ops Division
  - DITCO NCR
  - DITCO Pacific
  - DITCO Scott
  - DITCO Europe