

# **Fiscal Year 2024 Budget Estimates**

## **Defense Information Systems Agency**



**March 2023**

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**Operation and Maintenance, Defense-Wide Summary (\$ in Thousands)  
Budget Activity (BA) 4: Administration and Service-wide Activities**

	<u>FY 2022 Actuals</u>	<u>Price Change</u>	<u>Program Change</u>	<u>FY 2023 Enacted</u>	<u>Price Change</u>	<u>Program Change</u>	<u>FY 2024 Estimate</u>
DISA	2,044,836	51,828	154,628	2,251,292	68,403	248,004	2,567,698

**I. Description of Operations Financed:**

The Defense Information Systems Agency (DISA) is a combat support agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to the joint warfighters, National level leaders, and other missions and coalition partners across the full spectrum of operations. The DISA implements the Secretary of Defense's Defense Planning Guidance (DPG) and reflects the Department of Defense Chief Information Officer's (DoD CIO) Capability Programming Guidance (CPG). As noted in the DISA's Strategic plan, the DISA's mission is to conduct DoD Information Network (DoDIN) operations for the joint warfighter to enable lethality across all warfighting domains in defense of our nation. The DISA plans, engineers, acquires, tests, fields, operates, and assures information-sharing capabilities, command and control solutions, and a global enterprise infrastructure to support the DoD and national-level leadership.

The DISA serves the needs of the President, Vice President, Secretary of Defense, Joint Chiefs of Staff, COCOMs, and other DoD components during peace and war. The DISA provides networks, computing infrastructure, and enterprise services to support information sharing and decision making for the Nation's warfighters and those who support them in the defense of the nation. The DISA is committed to advancing new technologies in accordance with the National Defense Strategy to strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. Cyber, National Leadership Command Capability (NLCC), and the White House support are priority areas.

The Agency's efforts are structured around five strategic goals:

**Prioritize Command and Control (C2)** – Information is a critical C2 enabler for warfighters and mission partners. Our agency continues to address the capability and service needs of the warfighter through global mission partner engagement and information sharing. To achieve the Department's Joint All-Domain Command and Control (JADC2) vision, the DISA will streamline C2. This, combined with our cyberspace operations and cybersecurity situational awareness unities of effort, enable warfighters to make mission-based, real-time decisions at the tactical edge. Our work makes Presidential and senior leader communications, continuity of operations and government communications, and Nuclear Command, Control and Communications possible.

**Drive Force Readiness Through Innovation** – The DISA is driving implementation of next generation technology to ready DISA to address the future fight. The DISA will integrate these capabilities while leveraging industry best practices to efficiently adopt secure, enterprise-class technologies to facilitate real-time, mission-enabling solutions across different platforms, devices and classification levels. Much of our success

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

in this area comes through partnerships with industry and academia, and the use of innovative acquisition strategies.

**Leverage Data as A Center of Gravity** – As the DoD embraces several data-management initiatives, the DISA seek to build a culture that values data as a strategic asset to drive mission effectiveness. When thoughtfully collected and analyzed, data can accelerate innovation and improve service delivery. There is also an inherent power in owning data to control the high ground. The DISA’s Chief Data Officer (CDO) will drive the agency toward a more data-centric culture and ensure that data is discoverable, accessible and decision-enabling through secure and modernized systems, standards and governance.

**Harmonize Cybersecurity and The User Experience** - Our agency is on the leading edge of deploying, operating and sustaining cyber tools, capabilities and expertise to maximize DoDIN operations. The DISA is pursuing actions across the complete spectrum of domains, transport layers and technologies to enhance, standardize and centralize our threat-based defense of the cybersecurity environment. The DISA is actively aligning our efforts with a zero-trust security and software defined network architecture model to eliminate the traditional approach to identity management that is based on trusted or untrusted networks, devices and user credentials. Successful deployment of this model will achieve the DoD’s goals to integrate network and security solutions in the cloud and to enhance protections of end-user devices. The DISA will invest in commercial cloud capabilities to build enterprise identity and authentication solutions for DoD cloud environments to make data accessible to every owner from anywhere at any time.

**Empower the Workforce** – The DISA is a highly complex global organization, composed of military, civilian and government contractor personnel. The DISA recognize the importance of empowering and cultivating an innovative and diverse workforce through a framework that assures accountability, transparency and integrity with military and civilian talent leading within every level of the organization. At the DISA, talent diversification is an important approach towards the different perspectives to enhance problem solving, innovation and service delivery. Our agency is focused on establishing a talent pipeline of high-caliber candidates to serve as the next generation cyber workforce. The DISA will continue to offer professional, leadership and personal growth opportunities to fully develop and retain highly motivated and qualified employees across the agency in support of the warfighter. The DISA recognize the positive impact that a well trained and equipped workforce has on organizational climate and morale and will focus on developing the next generation of leaders throughout the agency.

**COVID-19 has brought unprecedented challenges to the DISA and rapidly increased mobile computing needs.** With the majority of the DoD personnel teleworking for their protection, the DISA has enabled remote capabilities by accelerating the DoD Mobility Classified Capability, increasing non-classified Internetprotocol router network circuit capacity and Commercial Virtual Remote (CVR) capabilities, and accelerating contract awards like the antivirus home use program. The DISA enabled mission-critical access to classified capabilities by expanding the ability to support secure remote access and provisioning a range of devices to support users globally. The DISA increased capacity for enterprise services such as the DoD365 video service, outlook web access, and enterprise audio conferencing bridges in order to support the growth of teleworking by five to ten times more. The DISA will continue to make mobility a priority to make secure data access possible from any location.

To be effective in the current world environment, there must also be comprehensive and integrated cyber protection for this infrastructure. The DoD’s long-term cyber strategic approach is based on mutually reinforcing lines of effort to build a more lethal joint force, compete and deter in

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

cyberspace, expand alliances and partnerships, reform the department, and cultivate talent. The current cyber domain is a dynamic, complex, and contested battlespace constantly under attack by an ever-evolving array of highly competent adversaries. These malicious actors seek to leverage the characteristics of the cyber domain to their advantage and compromise our ability to operate effectively in cyberspace. In order to defend against these evolving threats, the DISA is pursuing actions across domains and transport layers that will enhance, standardize, and centralize the defense of our cybersecurity environment. The DISA wants to enhance the defensive architecture with a focus on defending against both external and internal attacks, detecting lateral movement, and fully incorporating a more robust Zero Trust Architecture in a synchronized and standardized defensive implementation.

The DISA aligns its program resource structure across seven mission areas. These mission areas reflect the DoD goals and represent the DISA's focus on executing its lines of operation:

**Transition to Net Centric Environment:** To create and strengthen the network environment to facilitate the DoD information sharing by making data continuously available in a trusted environment.

**Eliminate Bandwidth Constraints:** To build and sustain the DoDIN transport infrastructure that eliminates bandwidth constraints and rapidly surges to meet demands, whenever and wherever needed.

**DoDIN Network Operations and Defense:** To operate, protect, defend, and sustain the enterprise infrastructure and information sharing services; and enable Command and Control.

**Exploit the DoDIN for Improved Decision Making:** To build the DoD enterprise-wide capabilities for communities of interest, such as command and control, and combat support that exploit the DoDIN for improved decision-making.

**Deliver Capabilities Effectively/Efficiently:** To deliver capabilities, based on established requirements, more effectively, economically, and efficiently than the DISA does today.

**Special Mission Area:** To execute special missions to provide communications support required by the President as the Commander in Chief, including day-to-day management, fielding, operation and maintenance of communications and information technology.

**The DISA continues to use the Cost Allocation Model (CAM) to assign costs of shared services to products and services.** The CAM identifies the total cost of a program and avoids unintended subsidy to the Defense Working Capital Fund (DWCF), gains visibility insight into the cost and consumption of shared services and addresses efficiencies.

The CAM is the tool which DISA uses to allocate its shared services across the agency's portfolio of programs and component organizations on an evaluated basis and approved by our cost analysis staff. Examples of costs being allocated includes items such as utilities and building operations at the DISA complex, Fort Meade, MD; the Defense Finance and Accounting Services (DFAS) personnel support; and DISANet

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

internal Information Technology (IT) costs. The CAM tool organizes the DISA programs and component organizations into categories to which specific costs are applicable. For example, activities outside of the Fort Meade complex -- such as the Joint Interoperability Test Command (JITC) -- are not charged a share of the utilities and building operations at the DISA complex, Fort Meade, MD, though they are charged a share of the DFAS personnel support and DISANet internal IT costs. The United States Strategic Command (USSTRATCOM) Field Office, which is not at Fort Meade and gets its IT support from USSTRATCOM, would only be charged a share of the DFAS personnel support costs. Costs are allocated on the basis of a validated measure, such as number of civilian personnel administered (DFAS personnel support), or number of seats used (DISANet internal IT costs). These costs are allocated across both the appropriate general fund and the DWCF activities.

**Mission Area: Transition to Net Centric Environment (FY 2024: \$343,446 thousand)**

1. Department of Defense Information Network Engineering Services (DoDIN ES) (FY 2024: \$ 82,783 thousand): DISA, through the Network Engineering Services, supports the Department of Defense Information Network (DoDIN) with technical architectures, updates to interface standards, and modeling and simulation services. These services ensure performance monitoring, cost effective technical solutions, and interoperability across the enterprise. They maintain critical standards across the DoD, Services, and Agencies. DISA strives to update critical standards every two years while also continually enhancing its capabilities.

Ongoing efforts supported include:

- Promoting centralized technology policy, standards, and leadership across the organization. To support this, DISA conducts technology outreach such as weekly Technical Exchange Meetings (TEMs) with the DoD Chief Information Officer (CIO), federal agencies, and industry. The purpose of the weekly TEMs is to identify best practices, material solutions, mature capabilities, and enterprise services
- Performing security engineering and accreditation of products via the assessment capabilities within the Technology Analysis Center (TAC) lab environment. The TAC lab enables analysis of emerging technologies and the associated capabilities via flexible and rapidly reconfigurable environments. This allows for real and/or near real-time assessment, which ultimately provides faster delivery of leading-edge technologies to the warfighters and mission partners.
- Ensuring environmental support for technology solutions as they are transitioned to an operations and maintenance requirement.

The Modeling and simulation services provide analyses to inform DISA's and DoD's infrastructure services and applications, ensuring DISA and DoD capabilities are planned, implemented, and assessed to meet the performance objectives cost-efficiently. Modeling and simulation services provide predictive analysis, systems engineering, and End-to-End (E2E) analytical assessments to inform design and investment recommendations ensuring new capabilities meet warfighter mission requirements. Benefits of these capabilities include when the boundary defenses, also known as "the first line of protection against outside threats", changes due to increased traffic demands (i.e., during the COVID

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

response). Ongoing beneficiaries include the DoD CIO, the DISA Network Services Directorate, the DISA Enterprise Services Directorate, the Program Executive Office-Mission Assurance, the Defense Information Systems Network Command Center, and the Joint Communications Simulation System users in the DoD.

2. Net-Centric Enterprise Services (NCES) (FY 2024: \$ 168,657 thousand): The DISA, through NCES, enables information sharing by connecting people and systems with information to people and systems who require that information. The DISA provides a portfolio of critical enterprise collaboration services to the warfighter, business, and intelligence end-users on the Secret Internet Protocol (IP) Data network and the Sensitive but Unclassified (SBU) IP Data network. This enables a secured, agile, robust, dependable, interoperable data sharing environment for the Department of Defense (DoD).

This portfolio:

- Allows more than two million authorized DoD users to collaborate across the CCMDs, Services, Joint Staff, and Agencies using a suite of web-accessible collaboration capabilities.
- Provides a resilient and flexible infrastructure to enable a secure collaborative environment that facilitates information sharing across the DoD.
- Has a robust enterprise messaging service that distinguishes the producer from the consumer. This allows consumers to subscribe to information that supports their missions and allows producers to publish perishable and non-perishable data without having to specify recipients.
- Provides the user with flexibility to couple services in varying ways and provide access to web and application content, warfighter information, and critical data in a secure environment.
- Supports application rationalization efforts through identifying and prioritizing the legacy applications for modernization. This facilitates the transition of applications to cloud hosting environments (both commercial and DoD on premise solutions).
- The Defense Enterprise Office Solution (DEOS) is a DoD-wide enterprise cloud solution for common communication, collaboration, and productivity. It is secure, universally accessible, and enables the DoD to operate and fight worldwide.

The DEOS offers greater functionality and efficiency than legacy collaboration systems, and:

- Provides support to battlespace environments, creates a simpler defensible perimeter by reducing DoD's IT footprint, streamlines information access and data sharing across DoD, and strengthens DoD Cybersecurity posture.
- Integrates email, collaboration services, office automation, and content management in unclassified and classified environments.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

3. DoD Enterprise Cloud Computing Ecosystem (FY 2024: \$ 92,006 thousand): The DISA, through its Hosting and Compute Center (HaCC) provides industry-leading cloud hosting and computing capabilities to the Department of Defense (DoD), the Joint Force, and, ultimately, to the warfighter. These cloud capabilities enable DoD staff and the warfighter to secure mission-critical data accurately and efficiently, in any location. The Agency's DoD Enterprise Cloud Computing Ecosystem program drives readiness through innovation by providing best value hybrid cloud offerings. The current offerings include the Joint Warfighting Cloud Capability (JWCC), Cloud Accelerators, and Cloud Migration Support.

The JWCC, the portfolio's primary offering, is a multi-vendor, enterprise-wide acquisition vehicle that enables the DoD to acquire commercial cloud services directly from a commercial Cloud Service Provider. The JWCC delivers a first-of-its kind capability that encompasses the needs of the entire enterprise at every classification level and delivers cloud capabilities down to the warfighter and is the first enterprise contract vehicle available DoD-wide with this scope. The JWCC brings the power of the commercial cloud to the DoD, enabling initiatives such as Joint All-Domain Command and Control (JADC2) and Zero Trust (ZT) to increase the lethality of the Department. Once a DoD customer selects a commercial cloud option, the JWCC also provides additional layers of monitoring and cybersecurity.

The DISA also provides Cloud Accelerators and Migration support capabilities, which equip mission partners with the tools and skillsets needed to adopt cloud services. These are a set of innovative products that make ordering, provisioning, onboarding, securing, and managing cloud faster, cheaper, and easier. Current capabilities are DoD Cloud Infrastructure as Code which uses automation to accelerate cloud adoption in the form of baselines that build out cloud environments, the Account Tracking and Automation Tool, a cloud provisioning tool that enables the initial creation of accounts for mission owners across multiple cloud vendors at all classification levels; Vulcan, a suite of tools that helps DOD customers; and the DISA Acquisition Package Preparation System (DAPPS), a web-based interview tool that guides mission owners through the DOD acquisition process.

**Mission Area: Eliminate Bandwidth Constraints (FY 2024: \$ 438,537 thousand)**

1. Defense Information Systems Network (DISN) Enterprise Activities (EA) (FY 2024: \$ 309,334 thousand): The Defense Information Systems Network (DISN) is the Department of Defense's (DoD's) consolidated worldwide telecommunications infrastructure that provides end-to-end information transport for DoD operations to the warfighters and the Combatant Commanders with a robust Command, Control, Communications, Computers and Intelligence information long-haul transport infrastructure. The DISN, seamlessly spanning full spectrum from terrestrial to space and strategic to tactical domains, provides the interoperable telecommunications connectivity and value-added services required to plan, implement, and support all operational missions, anytime, and anywhere pushing DISN services to the edge of the communications network. The DISN delivers an integrated platform consisting of DoD's core communications, computing, and information services, as well as integrating terrestrial, subsea, wireless, and satellite communications into a network cloud that is survivable and dynamically scalable. Operation and Maintenance funding primarily supports Air borne, Intelligence, Surveillance and Reconnaissance (AISR), Unified Video Dissemination System (UVDS), the Defense Red Switch Network (DRSN), the Enhanced Pentagon Capability (EPC)/Survivable Emergency Conferencing Network (SECN), IP enabling, and other key Senior leadership Communications voice and data communications. Continual enhancement of the DISN is needed to provide optimal network resources to the warfighter.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

Major DISN capabilities supported by appropriated funding include:

**Interoperability and Internet Protocol (IP) Enabling.** The DISN interoperability is responsible for integration of voice, video, and/or data services delivered ubiquitously across an interoperable, secure, and highly available IP network infrastructure. The IP enabling provides management and registration of all IP number resources for the DoD and is recognized as the DoD agent for IP number management with external internet governance organizations. It is also responsible for planning, managing, and sustaining delivery of Domain Name System (DNS) capabilities for the global Internet and for the classified and unclassified IP. In addition, it provides the “Who Is” capability for database queries relating to IP number registrations and .MIL domain information for the benefit of the DoD and the intelligence community organizations. The DISA continues to enhance IP capabilities by converting to a global converged infrastructure through IP version 6, where fault isolation and dynamic routing of network traffic enable enhanced service delivery and prevent service interruption to the end user.

**Defense Red Switch Network (DRSN).** The DRSN is a global, secure voice service providing the President, the Secretary of Defense, the Joint Chiefs of Staff, the Combatant Commands (COCOMs) and selected agencies with Nuclear Command, Control, and Communications (NC3) secure voice and voice conferencing capabilities up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level. The DRSN consists of Military Department and Agency-owned secure voice switches connected by a DISA provided transport backbone.

The AISR and UVDS efforts directly supports the Combatant Commanders/Services Agencies (CC/S/A) to gather, analyze and stream A-ISR sensor data to globally dispersed strategic, operational, and tactical customers. This timely and assured delivery of fused intelligence allows information superiority in support of Counterterrorism, Theater Campaign Plans and Contingency Operations.

**2. Defense Spectrum Organization (DSO) (formerly called Joint Spectrum Center) (FY 2024: \$ 44,335 thousand):** The Defense Spectrum Organization (DSO) is leading efforts to modernize Electromagnetic Spectrum (EMS) management software capabilities and services. The EMS enables warfighters to use critical technologies such as radar, navigation, connected weapons and sensors. DSO software capabilities and engineering analysis services mitigate negative effects from harmful interference and enable friendly forces to gain and maintain advantages in decision making. DSO capabilities also allow friendly forces access to the spectrum for operations. Access to the radio frequency portion of the EMS plays a critical role in national security and is fundamental to all the U.S. and coalition military operations to ensure the Warfighter has near real-time electromagnetic spectrum data to support operational requirements.

The DSO mission is integral to vital activities such as information operations, electronic warfare, and other Joint Staff directed projects. In support of the mission, the DSO:

- Provides data services and analytics for full electromagnetic situational awareness. This provides users the ability to visualize the electromagnetic environment, configure their own operational picture, and enable decision support and Joint All Domain Command and Control (JADC2).
- Improves DoD spectrum data quality to enable Artificial Intelligence/Machine Learning (AI/ML) and to support software



**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

deliveries that enable access to the EMS and mitigate interference to friendly data links.

- Supports the Joint Spectrum Interference Resolution (JSIR) program, which provides capabilities to report electromagnetic spectrum interference and coordinate mitigation procedures through the JSIR-O (JSIR Online) system. Includes reach-back analysis and support to mitigate interference to critical strategic national defense systems and data links.
- Creates architecture products for reference and to guide capability development to enable interoperability across the DoD and support the DoD in the national spectrum sharing initiatives.

3. Defense Information Systems Network (DISN) Infrastructure Services (formerly called DISN Subscription) (FY 2024: \$ 25,999 thousand): The DISA, through DISN, provides key infrastructure services required by the warfighter for day-to-day IT functionality such as secure voice, video, and data services. The secure voice and video services operate on both the classified and unclassified networks and incorporate security requirements unique to the military into commercially competitive services. The Global Content Delivery Services, which utilize a global fiber optic network for information transfer, are a key component of these services. By leveraging commercial Internet technology, the Global Content Delivery Services can accelerate, secure, and centralize DoD Web content and applications across the DISN. The centralization of these services incorporates network support and management. The capabilities provided by DISN are crucial to providing the warfighter with continuous, reliable, and secure voice, video, and data services at the speed of the mission.

4. DoD Teleport Program (FY 2024: \$ 32,695 thousand): The DoD Teleport, an Acquisition Category III program, acquires and modernizes satellite communications (SATCOM) capabilities that provide long-term variety of communications interfaces between the Defense Information System Network (DISN) terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence. The DoD Teleport System provides deployed warfighters with multiband, multimedia, and worldwide reach-back capabilities to DISN services through interoperability between multiple SATCOM systems and deployed warfighter tactical networks at seven Joint SATCOM Gateways located in California, Hawaii, Virginia, Bahrain, Germany, Italy, Japan, and fielding underway to establish a new DoD Teleport System in Australia.

The DoD Teleport program delivers capabilities using a multi-phased, 3-generation approach. Each generation delivers capabilities that provide warfighter coverage on a worldwide, regional, interregional and theater basis and the capacity to provide DISN, legacy tactical C4I services, and SATCOM throughput anywhere, anytime in support of support air, land, sea, and space operations critical to U.S. national security.

5. Standardized Tactical Entry Point (STEP) (FY 2024: \$ 9,514 thousand): The Standardized Tactical Entry Point (STEP) program is a suite of DoD Satellite Communications (SATCOM) Gateways that links deployed tactical users to the Defense Information System Network (DISN). Through the Defense Satellite Communications System (DSCS), STEP provides multi-media telecommunications services at extremely high throughput for deployed forces during operations and exercises. This program is vital to ensure the tactical users' access to the DISN services. The STEP program provides centralized integration capabilities, contingency capacity, and the necessary interfaces to meet the Combatant Commands (COCOMs), Services, and Agency requirements to support world-wide operations.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

6. 4TH Estate Network Optimization (4ENO) (FY 2024: \$ 16,660 thousand): The Fourth Estate Network Optimization Program Office, address physical security requirements and workplace productivity for users under the Department of Defense Network.

**Mission Area: DoDIN Network Operations and Defense (FY 2024: \$ 233,009 thousand)**

1. Field Commands and Field Offices (FY 2024: \$ 150,999 thousand): The DISA Field Commands and Field Offices (FC/FO) ensure that DISA's Joint Information Environment (spanning voice, video and data services) aligns to the Joint Cyber Warfighting Architecture (JCWA) and fulfill global warfighter needs in all phases of conflict. It is important to align to JCWA framework to collect, collate, and process intelligence to provide situational awareness for leadership and enable effective employment of battle Management Systems. FC/FO supports Combatant Commander and Combatant Command (CCMD) staff and integration of DISA services within the Joint All Domain Operations (JADO) Operational Plans (OPLANS).

FC/FO addresses the National Defense Strategy (NDS) priorities to deter aggression, while being prepared to prevail in conflict when necessary. This includes the prioritization of the PRC challenge in the Indo-Pacific. Sustaining a resilient Joint Force and defense ecosystem requires ongoing Information Technology (IT) services, facility/space accommodations, and programmatic operational support at eleven CCMD and National Military Command Center (NMCC) Head Quarters (HQ) location world-wide. Additionally, FC/FO aligns effective and on-site strategic Command and Control (C2) and situational awareness between the CCMD, Service Components, Agencies, and deployed forces. FC/FO supports National Security by:

- Preparing and publishing the DISA support plans for all the CCMD Theater Campaign Plans (TCP), global campaign plans and contingency plans.
- Reviewing and recommending DISA service improvements to more than 50 OPLANS annually.
- Providing customer service support and requirements advocacy to all stakeholders who subscribe, or plan to subscribe, to the DISA's existing or emerging information products and services. Enabling effective coordination and information exchange in support of the Services, policy, planning, and new capabilities.
- Developing the Joint All Domain Operations (JADO) / Information Environment (JIE) by assigning DISA FC/FO employee specialists to each CCMD HQ facility world-wide.
- Developing solutions to specific warfighting capability gap requirements identified in the Integrated Priority Lists (IPLs) for the Chairman of the Joint Chief of Staff.
- Defending the DoDIN by assuring system and network availability, information delivery, and information protection across strategic, operational, and tactical boundaries in support of the DoD, CCMD, Services, Agencies and the Joint Staff.
- Actively participating in Joint and coalition exercises.
- Conducting assessments of the threat and hazards, vulnerability, and risk to the DoD owned Defense Critical Infrastructure (DCI) and the inter/intra-dependencies needed to accomplish the required DoD missions in accordance with

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

the Department of Defense Directive (DoDD) 3020.40, DoD Policy and Responsibilities for Critical Infrastructure.

- Assessing critical Command, Control, Computer, Communication, Intelligence, Surveillance and Reconnaissance (C4ISR) components and capabilities during combat operations, even under service delivery constraints. Work is done via the Critical Infrastructure Program (CIP) which identifies, labels, and prioritizes the DoDIN sector and DISA assets
- Developing Continuity of Operations (COOP) plans and exercises to ensure that essential functions and operations will continue throughout wide range of threats, contingency operations and humanitarian disasters.

Additional missions include:

- Indonesian Pacific Combatant Command (Indo-Pacific) coalition partners and North Atlantic Treaty Organization (NATO) Field Offices ensure the U.S./Indo-Pacific/NATO partnership is considered in all planning and design efforts to facilitate C4ISR interoperability. The program is prioritizing the NDS challenges and is prepared to deter aggression and overcome conflict in the Indo-Pacific.
- Provide support to the Indo-Pacific coalition partners and NATO Ministry of Communications and Information Technology (MCIT) for transforming the Information and Communication Technology (ICT) in support of the business stabilization mission, while also encouraging strategic economic growth in other areas of operational responsibility (AOR).

2. Network Operations (NetOps) (FY 2024: \$ 51,649 thousand): The DISA NetOps program ensures that the Department of Defense Information Systems Network (DISN) capabilities, access points, and boundary protections meet DoD mission requirements. Through technical refresh, development, and sustainment, the DISA improves the DISN to achieve end-to-end interoperability.

The DISA provides continuous DODIN operational service delivery in 42 countries around the world and includes all Combatant Command and Service Component Operation centers across United States global military operations. DISA NetOps also delivers continuous situational awareness and ensures DODIN resilience. By fulfilling these duties, the DISA NetOps program mitigates service interruptions, develops alternate configurations, and provides enhanced mission support.

The DISA also supports the United States Cyber Command (USCYBERCOM) in its mission to provide secure, interoperable, and reliable operations across the DODIN within the Joint Cyber Warfighting Architecture (JCWA). DISA's primary tasks in this capacity are:

- Operating and defending the DoDIN Transport, which enables the DoD Enterprise services support to the USCYBERCOM internal and external Cyberspace Operations (CO), the Department of Defense Cyber Operations Forces (DoD COF) the Defensive Cyber Operations (DCO), and DoDIN Operations (DO).
- Enabling and conducting the actions necessary to provide certification, threat identification, intrusion prevention, intrusion detection, and incident response/recovery of both the Non-secured Internet Protocol Router Network (NIPRNet) and the

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

Secret Internet Protocol Router Network (SIPRNet).

- Providing the Command and Control (C2), situational awareness, and defense of the DoDIN and Enterprise services across all levels of command: strategic, operational and tactical boundaries in a contested battlespace.
- Supporting the DoD's full spectrum of war fighting to include support for intelligence and business missions.

The DISA executes its C2 mission to plan, direct, coordinate, integrate, and synchronize DO and DCO globally. More specifically, the DISA:

- Delivers reliable services worldwide in 42 countries at 3,800 locations.
- Manages and executes approximately 200 million managed network assets, in excess of 50,000 Telecommunications Service Orders (TSO) and circuit actions, 40,000 servers hosting 870 user applications, 17,000 circuits, 55 Satellite Communication (SATCOM) gateways, 38 petabytes of storage, 4.5 million DoD identities, 1.6 million to 4.5 million enterprise users, 1 million to 4.5 million mobility/voice/video/data over Internet Protocol (IP) users.
- Reports blockage and/or tracking of an average of 380 million malicious events per month.

Increasing cyber security threats have expanded the program's CO mission, both in terms of the breadth (e.g., Enterprise Services) and required depth of defenses in the DO/DCO mission space. The DISA supports USCYBERCOM's mission to direct, synchronize, coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. DISA is uniquely capable of meeting this requirement by leveraging the existing enterprise infrastructure.

**3. Joint Staff Support Center (JSSC) (FY 2024: \$ 30,361 thousand):** The JSSC provides 24x7 Command and Control (C2), Nuclear Command and Control (NC2), and National Military Command and Control (NMC2) operational and communications support. The JSSC supports the President, Secretary of Defense (SecDef), Chairman of the Joint Chiefs of Staff (CJCS), Joint Staff (JS), Combatant Commanders, and other National-level leaders through global maintenance of the Joint C2 and NC2 systems and cybersecurity oversight. In accordance with CJCS Operating Order (OPOR) 6-19 and CJCS Instruction (CJCSI) 3280.01E "National Military Command System", the JSSC Director provides operational direction for command, control, and communications (C3) support to create a mission-capable National Military Command Center (NMCC). These efforts enable the NMCC to perform National Military Command System (NMCS) seven mission essential functions (MEFs) and twenty-five mission essential tasks (METs). The JSSC oversees a critical decision support system for the NMCC and the National Joint Operations-Intelligence Center in the Pentagon and at Site R. By deterring strategic attacks against the United States, Allies, and partners through 24x7 support, the JSSC advances and safeguards vital U.S. national interests.

The JSSC provides 24x7 monitoring of the NMCC and alternate NMCC (NMCC-A) locations. The JSSC provides nuclear support operations for C2, communications, computer, and intelligence systems for worldwide situational monitoring, rapid decision-making, and force direction. Operational services support strategic threat operational warning, crisis management, situational awareness, course of action development, and national senior leadership decision-making. The JSSC provides these capabilities by sustaining the Global Command and Control System-

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

Joint (GCCS-J), Processing and Display System-Migration (PDS-M), Nuclear Planning and Execution System (NPES) and other systems. The JSSC sustains these capabilities for the Pentagon and Site R to ensure continuity of operations. The JSSC has aligned priorities to meet performance goals of the National Defense Strategy (NDS) to ensure a secure, reliable, and effective nuclear command, control, and communication (NC3) system by building a resilient Joint Force and defense ecosystem.

The JSSC also provides full-service television production and multimedia support to the SecDef, the CJCS, JS, and other DoD agencies, per requests from Pentagon organizations. These types of media include remote video and audio recordings, electronic graphics, video teleconferencing guidance, and operation of the NMCC secure television system. In addition, the JSSC provides tactical, operational, strategic, and collaborative planning support for various JS IT initiatives such as the NMCC IT Working Group (NIWG) and the JS IT migration. Personnel also assist the Joint Staff Hampton Roads, JS Pentagon, and other regional mission partners as they transition their IT services to the DISA-based offerings.

**Mission Area: Exploit the DoDIN for Improved Decision Making (FY 2024: \$ 1,015,935 thousand)**

1. Joint Service Provider (JSP) (FY 2024: \$ 580,232 thousand): The Joint Service Provider (JSP), under the DISA, is the exclusive Information Technology (IT) service provider for over 30 facilities and a wide variety of Department of Defense (DoD) personnel throughout the Pentagon Reservation and National Capital Region (NCR). JSP provides infrastructure network support, application support, data storage management, defensive cyber operations, cyber security compliance, and customer service support to critical DoD facilities. JSP serves over 40,000 customers spanning the Office of the Secretary of Defense (OSD), Washington Headquarters Services (WHS), Army, Joint Staff, and additional on-boarded customers.

The JSP IT program provides end-user computing capabilities needed to fulfill component missions. The JSP IT program includes DoD local area networks, computer servers, network storage subsystems, workstations, and desktop applications for processing information at all classification levels on over 110,000 end-user devices. By maintaining IT infrastructure for all key facilities and personnel, the JSP enables maximum mission effectiveness for all DoD IT users throughout the NCR.

JSP also encompasses the Secretary of Defense Communications Office (SECDEFCOMS). DoD guidelines require that the Secretary of Defense (SecDef) have resilient communication and situational awareness capabilities at the Pentagon. The SecDef also requires access to fully equipped alternative operating facilities and mobile communications during transit between facilities. SECDEFCOMS provides the SecDef these capabilities, which enable the SecDef and his Immediate Office to coordinate national defense, in every scenario.

2. Senior Leadership Enterprise (SLE)/Logistics Support Activities (LSA) (FY 2024: \$ 293,229 thousand): This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.

3. Combined Advanced Applications (FY 2024: \$ 62,855 thousand): This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

4. Global Command and Control System-Joint (GCCS-J) (FY 2024: \$ 29,369 thousand): The DISA provides the Global Command and Control System-Joint (GCCS-J), which is the Joint Command and Control (C2) system of record. It is an essential component for successful implementation of the operational concepts such as dominant maneuver, precision engagement, full-dimension protection, and focused logistics. The GCCS-J also directly supports the National Defense Strategy (NDS) priority of building a resilient Joint Force and defense ecosystem. The GCCS-J incorporates the core planning and assessment tools required by Combatant Commanders (COCOMs), their subordinates, and the Joint Task Force (JTF) Commanders to support the readiness of the Services requirements.

The GCCS-J provides critical C2 capabilities to the Commander-in-Chief, Secretary of Defense, National Military Command Center, Combatant Commands (CCMDs), Joint Force Commanders, and Service Component Commanders. GCCS-J users include decision makers at the strategic national, theater, operational levels, and all CCMDs at sites around the world.

The GCCS-J capabilities include:

- Integrated, near real-time picture of the battlespace to support joint operations on US and coalition networks.
- Air, maritime, ground, space and cyber tracks for US, coalition, and enemy forces.
- Applications for situational awareness, missile warning, intelligence, targeting, imagery exploitation, and applications for modeling chemical, biological, radiological, and nuclear (CBRN) hazard areas and effects.
- 24x7 support to DoD components around the globe. Support efforts include:
  - Global Tier II technical support to over 660 sites
  - Operational monitoring and reporting of 53 critical sites
  - Global Common Operational Picture (G-COP) technical support and management of National Capital Region (NCR) Global COP servers
  - Tier I and II technical support of 6 JOPES Strategic Server Enclaves (SSEs) and Deployable Strategic Server Enclaves (DSSEs)

5. Other Programs (FY 2024: \$ 20,636 thousand): The funding associated with other programs is primarily for the infrastructure costs for the DISA's interoperability facility in the National Capital Region.

6. National Military Command System (NMCS) (FY 2024: \$ 177 thousand): The National Military Command System (NMCS) provides the President, the Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff, the National Military Command Center (NMCC), the NMCC Site R, and the executive travel fleet with the ability to execute C2 over all the U.S. military forces across the full spectrum of threats/contingencies. The NMCS engineering projects support the DISA's mission of providing responsive, timely, and accurate information to the warfighter.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

7. Joint Planning and Execution Services (JPES) (FY 2024: \$ 29,437 thousand): The DISA, through the Joint Planning & Execution Services (JPES) Program Management Office (PMO), provides IT capabilities to support the Department of Defense's Joint Planning Process (JPP). These capabilities support force planning, deployment planning, allocation of forces, execution, and Global Force Management (GFM) processes for military operations as part of the Joint Command & Control (JC2) mission.

In FY 2024 the JPES program maintains and sustains three operational systems with O&M funding:

- Joint Operations Planning and Execution System (JOPES) - The critical Joint Command and Control system that provides automated force planning and execution capabilities necessary for simultaneous and resource-informed planning activities. The JOPES supports thousands of operational users across the globe. Additionally, there are 18 external systems across the Combatant Commands (CCMDs), Military Services, and Defense Agencies that are dependent on JOPES to perform force planning, deployment planning and execution activities.
- Joint Capabilities Requirements Manager (JCRM) - A web-based application and database. It enables the Global Force Management Allocation Process (GFMAP) for CCMDs to draft, staff, store, and submit force requirements for ongoing and emerging military operations, contingency plans, and military exercises worldwide. JCRM is vital to managing complex global force requirements and tracking the distribution of U.S. military forces among the CCMDs. There is no alternate capability to fulfill the JCRM mission.
- Joint Collaboration Tool (JCT) - Serves as a secure messaging system that CCMDs, Military Services, and Lift Providers use to collaborate and communicate when accessing JOPES and JCRM to support military requirements, operations, and exercises worldwide. Additionally, JCT enables cybersecurity updates to protect against cybersecurity threats.

**Mission Area: Deliver Capabilities Effectively/Efficiently (FY 2024: \$ 203,635 thousand)**

1. Shared Services Units/Program Executive Offices (FY 2024: \$ 130,008 thousand): This activity funds foundational operating capabilities for the DISA, such as financial management, information technology, strategic planning, manpower/personnel security, and acquisition products and services to all agency programs and business areas world-wide. The DISA is actively working to develop modern technical solutions to support improvements in order provisioning, contract provisioning, human-resource, and financial functions.

2. Management Headquarters (FY 2024: \$ 41,052 thousand): The management headquarters funding is utilized for salaries and operating expenses associated with the command and executive staff and their key control organizations, which provide oversight, direction, and control of the DISA activities. The command and executive staffs enable the DISA to continuously operate and assure a global net-centric enterprise in direct support to the joint warfighter, national level leaders, and other mission and coalition partners across the full spectrum of operations. To strengthen workforce engagement and motivation, the DISA has developed several new and exciting initiatives that are specifically designed to empower the workforce to take an active role in process and cultural change. These include a trust and accountability framework, a climate

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

synergy group aimed at boosting workforce morale and retention, coaching, mentoring, and team building trainings.

3. Pentagon Reservation Maintenance Revolving Fund (PRMRF) (FY 2024: \$ 32,575 thousand): Section 2674 of title 10 United States Code, established the Pentagon Reservation Maintenance Revolving Fund (PRMRF) authorizing the Secretary of Defense to establish rates and collect charges for space, services, protection, maintenance, construction, repairs, and alterations of facilities provided at the Pentagon Reservation.

**Mission Area: Special Mission Area (FY 2024: \$ 333,136 thousand)**

1. White House Communications Agency (WHCA) (FY 2024: \$ 301,242 thousand): The WHCA is a joint service military agency under the operational control of the White House Military Office (WHMO) and under the administrative control of the DISA. All mission operations are in accordance with the National Defense Authorization Act (NDAA) of 2006, Public Law 109-163. The WHCA provides 24/7 worldwide classified and unclassified information services to the President, Vice President, WHMO and others as directed by the President via the White House Director of Technology. These services equip the President and other key leaders with the information needed to decide on and communicate about high-level national security challenges. The WHCA primarily operates in the National Capital Region but also supports the Presidential Information Technology Community (PITC) networks at Camp David, second residences, various worldwide travel sites and other Executive of the President (EOP) and WHMO offices as well as in vehicles and aircraft. WHCA also supports alternate sites for Continuity of Operations (COOP) and Continuity of Government (COG), the Signal Support Element (SSE) and other Head of State (HoS) in specific designated locations. This enables unified communications and provides leaders the ability to communicate during emergency situations. The WHCA ensures that the president can communicate with anyone in the world at any time and location.

In addition, the Agency is now responsible, under Presidential direction, to maintain the Crisis Management System (CMS). Through the CMS, the DISA provides state-of-the-art Top Secret Sensitive Compartmented Information (TS/SCI) and Extremely Sensitive Information (ESI) voice and video teleconferencing services to the President and other national security leaders.

2. White House Situation Support Staff (WHSSS) (FY 2024: \$ 30,497 thousand): The DISA, through the White House Situation Support Staff (WHSSS), provides key financial and personnel resources under Presidential direction. The WHSSS supports critical information technology and communication services for the National Security Council (NSC), including those performed by the White House Situation Room (WHSR).

WHSR provides 24/7 global situational awareness, crisis management facilitation, emergency action support, and executive communications for the President of the United States (POTUS) in his roles as Commander-in-Chief of the Armed Forces, Head of State, and Chief Executive. WHSR also supports the Vice President of the United States (VPOTUS), National Security Advisor, NSC staff, and select senior White House staff directly.

The DISA provides applications and tools that support WHSR watch floor operations and NSC decision making, and Presidential Records Management. The WHSR serves a unique network communication and integration function that provides integrated communication



**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**I. Description of Operations Financed: (Cont.)**

capabilities for over ten (10) classified video and audio networks. Personnel oversee operations and maintenance of communications systems and are also deployed to alternate locations to assist with Continuity of Operations (COOP) and Continuity of Government (COG), providing WHSR global support during special travel missions and national emergencies. Finally, WHSSS personnel oversee budgeting, acquisition, logistics and administrative activities required to execute COOP, COG, and special mission travel.

3. Communications Management Control Activity (CMCA) (FY 2024: \$ 1,397 thousand): The CMCA provides communications support to the United States SecretService (USSS) for the Presidential campaigns, as well as for dignitary protective duties. The CMCA also supports the Joint Staff/J6, Joint Directorate of Military Support (JDOMS) for special events. Public Law 106-544 assigned the USSS responsibility for coordinating, planning, exercising, and implementing security for the National Special Security Events (NSSE). Additionally, the DoD Directive 3025.13 mandated that the DISA provides the CMCA Headquarters with operations and maintenance funding.

4. Crisis Management System (CMS) (FY 2024: \$0 thousand): The DISA is responsible, under Presidential direction, to build, operate, secure, and maintain CMS which provides state-of-the-art Top Secret Sensitive Compartmented Information (TS/SCI), Special Access Program (SAP), and Extremely Sensitive Information (ESI) secure voice and video teleconferencing and facsimile services to the President, Vice President, Executive Office of the President (EOP), Cabinet Members, various key national security leaders and agency operations centers, and alternate sites supporting Continuity of Operations (COOP) and Continuity of Government (COG). The system has a “no fail” mission with the ability to function in ground, mobile, and airborne modes for exchange of time-sensitive critical information for both day-to-day and crisis operations regardless of location.

The CMS, funding provides maintenance, configuration management, certification and accreditation activities including system security monitoring and testing, and engineering support. The system provides real-time Top Secret/Sensitive Compartmented Information (TS/SCI) secure video conference communications for the President and high-level advisors including multi-party calls between fixed and mobile sites for day-to-day and crisis operations.

**II. Force Structure Summary:**

N/A

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands)**

	<b>FY 2022 Actuals</b>	<b>Budget Request</b>	<b>FY 2023 Congressional Action</b>		<b>Appropriated</b>	<b>Current Enacted</b>	<b>FY 2024 Estimate</b>
			<b>Amount</b>	<b>Percent</b>			
<b>A. BA Subactivities</b>							
1. Transition to Net Centric Environment	\$151,496	\$309,621	\$-1,387	-0.45%	\$308,234	\$308,234	\$343,446
2. Eliminate Bandwidth Constraints	\$263,682	\$279,540	\$7,837	2.80%	\$287,377	\$287,377	\$438,537
3. DODIN Network Operations	\$218,802	\$226,502	\$-11,776	-5.20%	\$214,726	\$214,726	\$233,009
4. Exploit the DODIN for Improved Decision Making	\$986,424	\$955,486	\$-15,123	-1.58%	\$940,363	\$940,363	\$1,015,935
5. Deliver Capabilities Effectively/Efficiently	\$143,171	\$173,806	\$5,012	2.88%	\$178,818	\$178,818	\$203,635
6. Special Missions	\$281,261	\$321,774	\$0	0.00%	\$321,774	\$321,774	\$333,136
<b>Total</b>	<b>\$2,044,836</b>	<b>\$2,266,729</b>	<b>\$-15,437</b>	<b>-0.68%</b>	<b>\$2,251,292</b>	<b>\$2,251,292</b>	<b>\$2,567,698</b>

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

<b><u>B. Reconciliation Summary</u></b>	<b><u>Change FY 2023/FY 2023</u></b>	<b><u>Change FY 2023/FY 2024</u></b>
<b>BASELINE FUNDING</b>	<b>\$2,266,729</b>	<b>\$2,251,292</b>
Congressional Adjustments (Distributed)	-15,000	
Congressional Adjustments (Undistributed)	0	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	-437	
<b>SUBTOTAL APPROPRIATED AMOUNT</b>	<b>2,251,292</b>	
Fact-of-Life Changes (2023 to 2023 Only)	0	
<b>SUBTOTAL BASELINE FUNDING</b>	<b>2,251,292</b>	
Supplemental	0	
Reprogrammings	0	
Price Changes		68,403
Functional Transfers		0
Program Changes		248,003
<b>CURRENT ESTIMATE</b>	<b>2,251,292</b>	<b>2,567,698</b>
Less: Supplemental	0	
<b>NORMALIZED CURRENT ESTIMATE</b>	<b>\$2,251,292</b>	<b>\$2,567,698</b>

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

<b>FY 2023 President's Budget Request (Amended, if applicable)</b> .....	<b>\$2,266,729</b>
1. Congressional Adjustments .....	\$-15,437
a) Distributed Adjustments.....	\$-15,000
1) Program decrease unaccounted for .....	\$-17,000
2) Program Increase - Army Led Interagency Critical Infrastructure Protection Training .....	\$2,000
b) Undistributed Adjustments.....	\$0
c) Adjustments to Meet Congressional Intent.....	\$0
d) General Provisions .....	\$-437
1) Federally Funded Research and Development Center (FFRDC) Reductions (Sec. 8026) .....	\$-437
<b>FY 2023 Appropriated Amount</b> .....	<b>\$2,251,292</b>
2. Supplemental Appropriations .....	\$0
a) Supplemental Funding.....	\$0
3. Fact-of-Life Changes.....	\$0
a) Functional Transfers.....	\$0
b) Technical Adjustments .....	\$0

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

c) Emergent Requirements .....	\$0
<b>FY 2023 Baseline Funding</b> .....	<b>\$2,251,292</b>
4. Reprogrammings (Requiring 1415 Actions) .....	\$0
a) Increases .....	\$0
b) Decreases .....	\$0
<b>Revised FY 2023 Estimate</b> .....	<b>\$2,251,292</b>
5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings .....	\$0
a) Less: Supplemental Funding .....	\$0
<b>FY 2023 Normalized Current Estimate</b> .....	<b>\$2,251,292</b>
6. Price Change .....	\$68,403
7. Functional Transfers .....	\$0
a) Transfers In .....	\$0
b) Transfers Out .....	\$0
8. Program Increases .....	\$400,226
a) Annualization of New FY 2023 Program .....	\$0

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

b) One-Time FY 2024 Increases .....\$0

c) Program Growth in FY 2024 .....\$400,226

1) DoDIN Engineering Services..... \$6,345

The increase is for the Secret Internet Protocol Router Network (SIPRNet) Modernization which will work to improve the security and resiliency of the Department’s warfighting network. These capabilities will improve the security and defense of e-mail traffic, both within as well as external to SIPRNet. The funding is also for the modernization of Secret Internet Protocol Router (SIPR) Gray Network operational components, including the DoD Mobility Classified Capability-Secret (DMCC-S) gateways/stacks, the Gray Public Key Infrastructure (Gray PKI), and the DoD Public Key Infrastructure (DoD PKI). The funding covers technology insertion for operational performance enhancements, and the costs to improve operational systems reliability, maintainability, portability, and migration.  
(FY 2023 Baseline: \$68,499 thousand)

2) DoD Teleport Program ..... \$4,231

The increase is for the In-Service Engineering Agent (ISEA) support from the Naval Information Warfare Center-Atlantic (NIWC-Atlantic). The ISEA functions for the DoD Teleport Advanced Extremely High Frequency (AEHF), Extremely High Frequency (EHF), and ultra-high frequency (UHF) terminals and Mobile User Object System (MUOS) to Legacy UHF Gateway Component (MLGC) and MUOS Voice Gateway (MVG) includes the sustainment of fielded systems through End-of-Life (EOL) replacement, system upgrades, follow-on, or interrelated system, distant support, onsite repair, installations, and system analysis to ensure capabilities are performing within designed specifications and peak capabilities, including cybersecurity sustainment. The ISEA support spans across multiple terminals and MUOS Legacy Gateway Component (MLGC) and MVG systems across six Joint Enterprise SATCOM Gateways in California, Virginia, Hawaii, Bahrain, Germany, Italy, Japan and Joint SATCOM Engineering Center, and Aberdeen Proving Ground (APG). The Milestone Decision Information Systems Executive Agent (MDISEA) supports satellite communications (SATCOM) systems to the Warfighter across the Enterprise SATCOM Gateway (ESG) in support of the DoD Teleport Program. Without ISEA support, these systems are vulnerable to system outages and adversarial threats that translate into critical mission failures due to nonoperational SATCOM capabilities required for air, land, sea, and space operations critical to U.S. national security.  
(FY 2023 Baseline: \$26,157 thousand)

3) White House Communications Agency (WHCA) ..... \$24,549

Increase is due to the realignment of the Crisis Management System under the purview of the WHCA for a more centralized administration of all TS/SCI level communications supporting the President.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

(FY 2023 Baseline: \$267,125 thousand)

4) Field Commands and Field Offices ..... \$9,084

Increase will support the Regional Command Network Enhancement and Information Technology (IT) effort in providing Active Enterprise Network Operations: always on, continuously available operational and security capabilities, where a fault in a single location does not affect the ability of the DISA Global Operations Command to continue to perform seamlessly in another location with zero downtime. Specifically, the increase will upgrade existing facility equipment and end user equipment that is essential in meeting the Regional Commands core operational mission to provide, operate, and defend the DoDIN and its enterprise infrastructures and services. The increase will also be used for the Joint Mission Assurance Assessment requirements and Critical Infrastructure Protection Program support.

(FY 2023 Baseline: \$135,240 thousand)

5) Civilian Compensation..... \$17,823

An Increase of Direct FTEs reflects an internal rephasing of DISA's workforce. DISA continues its rephasing efforts that stemmed from its past decision to reduce its civilian FTE levels in under executing programs and instead, gradually rephase these FTEs in future budget years. The increase of Direct FTEs represents this year's rephasing levels. The DISA continues to use a variety of recruiting initiatives such as direct hiring authority, job fairs, cyber excepted service authorities, etc., to fulfill its budgeted manpower levels.

(FY 2023 Baseline: \$414,140 thousand; 2,461 FTEs; +83 FTEs)

6) Shared Services ..... \$24,226

Increase for additional DoD365 licenses to meet current staffing needs. This increase covers the DISANET and the DoDNET licensing, commodity IT, and Global service desk support for civilian, military, and contractor staff. The DISA is establishing centralized payment of this bill for transparency and management efficiency.

(FY 2023 Baseline: \$107,195 thousand)

7) Defense Information Systems Network (DISN) Enterprise Activities (EA) -DISN Transport ..... \$6,000

To increase the DISN Transport funding in support of a classified requirement.

(FY 2023 Baseline: \$183,272 thousand)

8) Defense Red Switch Network (DRSN) - (DISN EA)..... \$9,006

Increase will support sustain to the voice only DRSN and develops the follow-on system for MLV2 conference capability to maintain a comprehensive and effective continuity of operations capability for government and departmental senior leaders.

(FY 2023 Baseline: \$183,272 thousand; +22 FTEs)

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

<p>9) Logging Utility for Java (Log4j) - DISN EA, DoDIN ES, NetOps, Share Services .....</p> <p>Increase enhances the security of Log4j in FY24 to address cyber vulnerabilities across the Dept that were identified in Dec 2021 by monitoring, detecting and responding to malicious attacks and installing patches, in accordance with the DISA's mitigation plan.</p> <p>(FY 2023 Baseline: \$408,321 thousand)</p>	<p>\$33,533</p>
<p>10) OSD IT Enterprise - JSP .....</p> <p>Increase supports the modernization of JSP Help Desk, by funding new information technology tools which will improve the level of customer service provided by the JSP Help Desk.</p> <p>(FY 2023 Baseline: \$495,326 thousand)</p>	<p>\$12,000</p>
<p>11) Information Technology (IT) Technical Debt - 4ENO and JSP .....</p> <p>Buydown of IT Technical Debt; Increase is applied to technical debt, digital modernization, or cloud transition efforts. This investment will improve end-user experience.</p> <p>(FY 2023 Baseline: \$495,326 thousand)</p>	<p>\$33,323</p>
<p>12) Long Haul Communications - DISN EA.....</p> <p>This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.</p> <p>(FY 2023 Baseline: \$183,272 thousand)</p>	<p>\$100,000</p>
<p>13) Enhancement 365 Licensing for Improved Zero Trust - JSP, NCES, Shared Service .....</p> <p>Increase supports enhancement of DoD Microsoft 365 Enterprise Licensing for Improved Zero Trust Capabilities. Provides funding to purchase Microsoft 365 license upgrades for the DoD and conduct a study on the ability to extend Microsoft capabilities in all DoD 365 construct for Zero Trust Implementation across Non Secure Internet Protocol Router (NIPR).</p> <p>(FY 2023 Baseline: \$752,856 thousand)</p>	<p>\$32,951</p>
<p>14) Command and Control (C2) Senior Leadership - DISN EA .....</p> <p>This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.</p> <p>(FY 2023 Baseline: \$183,272 thousand)</p>	<p>\$9,900</p>
<p>15) Senior Leadership (SL) Enterprise - SLE .....</p> <p>This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.</p> <p>(FY 2023 Baseline: \$292,048 thousand)</p>	<p>\$33,750</p>
<p>16) JWICS Domain Transfer - JSP.....</p>	<p>\$15,023</p>



**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

Details provided for this program are submitted in appropriately classified DoD exhibits.  
(FY 2023 Baseline: \$495,326 thousand)

17) Expand and Sustain Standardized Monitoring - JSP ..... \$4,360  
Increase supports expansion and sustainment of standardized computer monitoring to establish a centralized monitoring capability on enterprise data platforms, building on Air Force pilot efforts.  
(FY 2023 Baseline: \$495,326 thousand)

18) Federal Contractors \$15 Per Hour - Shared Service ..... \$2,728  
Additional funding to address the estimated impacts of Executive Order (E.O.) 14026, Increasing the Minimum Wage for Federal Contractors, dated April 27, 2021. E.O. 14026, Section 4(a) requires the Department of Labor to implement regulations to increase the minimum wage to \$15 per hour by January 30, 2022, on contracts covered by the Fair Labor Standards Act, the Service Contract Act (SCA), or the Davis Bacon Act (DBA). The E.O. also applies only to Federal Contractors and Subcontractors on new contract actions entered into on or after January 30, 2022.  
(FY 2023 Baseline: \$107,195 thousand)

19) White House Communications Agency (WHCA) Conversion ..... \$4,326  
Increase supports increased mission to build, operate, monitor, train, and maintain the classified enterprise wide PITC-Secret and PITC-TS network.  
(FY 2023 Baseline: \$267,125 thousand; +24 FTEs)

20) Compensation and Benefits – One more Compensable Workday .....\$68  
One additional compensable day is included in FY 2024. The number of compensable days for FY 2023 is 260 days (2,080 hours), and for FY 2024 is 261 days (2,088 hours).  
(FY 2023 Baseline: \$414,140 thousand)

21) Program Increase (classified)..... \$17,000  
Details provided for this program are submitted in appropriately classified DoD exhibits.

9. Program Decreases .....	\$-152,223
a) Annualization of FY 2023 Program Decreases .....	\$0
b) One-Time FY 2023 Increases .....	\$-2,000

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

1) Program Increase - Army Led Interagency Critical Infrastructure Protection Training .....	\$-2,000
 c) Program Decreases in FY 2024 .....	 \$-150,223
1) Travel of Persons .....	\$-9,768
The decrease is attributed to reduced travel for the President's Elite Communications (PEC) unit during the Congressional Mid-term campaign travel by the President and Vice President of the United States. The PEC unit is comprised of highly motivated and trained Military members who often travel with the President and Vice President. (FY 2023 Baseline: \$36,750 thousand)	
2) Crisis Management System .....	\$-24,549
Decrease is due to the realignment of the Crisis Management System under the purview of the WHCA for a more centralized administration of all TS/SCI level communications supporting the President. (FY 2023 Baseline: \$24,549 thousand)	
3) Net Centric Enterprise Services (NCES).....	\$-18,044
Decrease is due to shift in purchases of Impact Level 6 (SIPRNet) licenses as well as the Identity Credentialing and Access Management (ICAM) Global Federated User Domain (GFUD) transitioning to Cyber. The GFUD is a new capability and enclave that is closely aligned with the Defense Enterprise Authentication Service (DEAS) system used to provide authentication of privileged users to the DoD Cloud-based systems and services. This is an extension and enhancement of the on-premise DISA DEAS system and will attempt to merge the two programs once administration and change management is aligned. (FY 2023 Baseline: \$150,335 thousand)	
4) Combined Advance Applications.....	\$-18,405
This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits. (FY 2023 Baseline: \$74,670 thousand)	
5) Network Operations.....	\$-2,283
The decrease is due to reductions in SATCOM costs related to the support of operational direction, control, and maintenance of the DISA enterprise infrastructure and services. (FY 2023 Baseline: \$49,265 thousand)	
6) Defense Spectrum Organization (DSO).....	\$-1,567

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**III. Financial Summary (\$ in Thousands) (Cont.)**

Decrease is due to a reduction in Contract support needed to develop Electromagnetic Battle Management (EMBM) capabilities that provide situational awareness and joint integration leveraging the Electronic Warfare Planning and Management Tool, the Joint Spectrum Data Repository and the GCCS-J.  
(FY 2023 Baseline: \$43,794 thousand)

7) Senior Leadership Enterprise (SLE)..... \$-35,000  
This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.  
(FY 2023 Baseline: \$292,048 thousand)

8) Logging Utility for Java (Log4j) - Network Operations (NetOps) and Shared Services ..... \$-33,188  
Decrease is due to a one-time increase in FY 2023 to support the Log4j Secure Internet Protocol Router Network (SIPRNet) Packet Flow capability, which provides views into network traffic and Internet Protocol (IP) to IP Connections. Log4J vulnerability exploitation and compromise is primarily discovered through network traffic. Federated Search provides DISA the ability to collect and analyze endpoint and network data from across the DISN and Cyber Security Service Program (CSSP) customer networks.  
(FY 2023 Baseline: \$156,460 thousand)

9) Defense Red Switch Network (DRSN) - (DISN EA)..... \$-7,419  
Decrease is due to a one-time increase in FY 2023 to support the sustainment of the DRSN through FY 2023, which includes the protection of Top Secret/Sensitive Compartmented Information (TS/SCI) level communications between the President of the United States (POTUS) and National Security Leadership when using the secure voice and voice conferencing capabilities.  
(FY 2023 Baseline: \$183,272 thousand)

**FY 2024 Budget Request..... \$2,567,698**

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**IV. Performance Criteria and Evaluation Summary:**

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
<p><u>Chief Information Officer:</u></p> <p>1. Declassification Review Metrics: Complete reviews for all referrals for equity within a 60-day period and make the required determinations for each document.</p> <p>2. Organizational Execution Plan (OEP)/Business Enterprise Architecture (BEA)/Business Capability Acquisition Cycle (BCAC): Report status of timely completion/submission – on a quarterly basis – of the DISA Chief Information Officer Organizational Execution Plan portfolio (and any execution-period changes) for the Pre-Certification Authority (number of submissions submitted timely against total number of submission that quarter).</p> <p>3. Compliance with Cybersecurity Workforce Professional and Certification: Periodic inspection of deliverable products and services - 8570 Compliance Team reports the qualification percentages of the Agency's Information Assurance workforce on a weekly basis determining if Information Assurance (IA) positions (civilian, military and contractor support personnel) have the appropriate DoD Baseline Certification to perform their assigned duties.</p> <p>4. Cyber Hygiene Scorecard: Weekly monitoring of the Host Based Security System, Patching and Configuration Statuses.</p>	<p>1. 100%</p> <p>2. 100%</p> <p>3. 100%</p> <p>4. 87%</p>	<p>1. 100% Quarterly</p> <p>2. 100% Quarterly</p> <p>3. 100% Quarterly</p> <p>4. 100% Quarterly</p>	<p>1. 100% Quarterly</p> <p>2. 100% Quarterly</p> <p>3. 100% Quarterly</p> <p>4. 95% Quarterly</p>
<p><u>Chief Data Officer:</u></p> <p>5. Data Stewardship Guide and Office Chief Data Officer Charter: Develop Data Stewardship Guide and Office Chief Data Officer Charter – Develop, implement, and maintain data management governance for the agency.</p> <p>6. Conduct annual DOD Knowledge Management Symposium: Develop and Deploy</p> <p>7. Department of Defense Enterprise Portal System (DEPS) Site to SharePoint Online (SPO) site migration: Migration of content.</p>	<p>5. 60%</p> <p>6. 100%</p> <p>7. 70%</p>	<p>5. 100%</p> <p>6. 100%</p> <p>7. 100%</p>	<p>5. 100%</p> <p>6. 100%</p> <p>7. 100%</p>

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**IV. Performance Criteria and Evaluation Summary:**

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
<u>Defense Information Systems Network (DISN) Infrastructure Services:</u> 8. Availability: Non-Secure Internet Protocol Network (NIPRNet) access circuit availability 9. Latency: Secure Internet Protocol Router Network (SIPRNet) latency (measurement of network delay). 10. Availability: Defense Red-Switch Network (DRSN) switch availability	8. 99.78% 9. 40.31 Milliseconds (within the continental U.S.) 10. ≥ 99.9%	8. > 98.5% 9. ≤ 100 Milliseconds 10. ≥ 99.9%	8. > 98.5% 9. ≤ 100 Milliseconds 10. ≥ 99.9%
<u>Department of Defense Information Network Engineering Services (DoDIN ES):</u> 11. Percentage of Spare Capacity: Maintain at least 25% spare capacity, to allow for provisioning of unforeseen requirements and rerouting under outages.	11. ≥ 40% for NIPR, SIPR, and Optical Transport	11. ≥ 25%	11. ≥ 25%
<u>Defense Info Infrastructure Engineering and Integration:</u> 12. Number of Engineering Artifacts: Total number of engineering artifacts adopted equal to or greater than 5 (≥ 5)	12. 5	12. 5	12. 5
<u>Joint Services Provider (JSP):</u> 13. Data Management: Maintain a data availability of 99% for enterprise applications and replicated data for unclassified and classified transport networks. 14. Systems Management: Provide availability for all JSP managed systems and services to include but not limited to Virtual Desktop Infrastructure (VDI), Active Directory, File/Print, and Elastic Sky X (ESX) Infrastructure. (≥99%). 15. Non-Classified Internet Protocol Router Network (NIPRNet) Continuous Monitoring: Asset visibility for compliance through continuous monitoring on the NIPRnet. 16. Ticket Resolution: 90% of Incident tickets shall be resolved within 8 business hours of Incident report. 17. Scan Rate: Scan every asset once per week with a minimum credentialed scan rate of 95%.	13. 99% availability 14. 99% availability 15. 83% 16. 93.5% 17. 97%	13. 99% availability 14. 99% availability 15. 83% 16. 90% 17. 95%	13. 99% availability 14. 99% availability 15. 83% 16. 90% 17. 95%

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**IV. Performance Criteria and Evaluation Summary:**

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
<u>Communications Management Control Activity (CMCA):</u> 18. Service Availability: Maintain 99.9% availability of the information and orders dissemination tool to the authorized users in a reliable, responsive, and timely manner at all times.	18. 99.99%	18. 99.9%	18. 99.9%
<u>DoD Teleport Program:</u> 19. System Availability: Utilizing two-in-view architecture, maintain 99% of global availability of Teleport systems.	19. 100%	19. 99%	19. 99%
<u>Secretary of Defense Communications:</u> 20. Critical Infrastructure (CI): Provide advanced mission-tolerant infrastructure, systems and support to the Immediate Office of the Secretary of Defense for a high availability, workstation-based, computer network. 21. Security Operations (SO): Provide communications, Information Technology (IT), and physical security in order to maintain full-scope Information Assurance (IA), Computer Network Defense (CND), and Incident Response (IR). 22. Communications Support: Delivery of select classified and unclassified customer communications, computing, and information services extended to the assigned aircraft, mobile platform, residential and travel site for the Immediate Office of the Secretary of Defense, crucial in his exercise of Command Control (C2) capabilities of the Department of Defense. 23. Continuity of Operations/Continuity of Government (COOP/COG): Serve as the single point of contact for all Secretary of Defense, Immediate Office COOP/COG and continuity of the Presidency matters including but not limited to Alternate Site Management and Operations, IT Disaster Recovery Planning, Official Travel Mission Contingency Planning, NC3 Planning and Implementation. 24. Enterprise Initiative, Test and Development: Support a variety of Research, Development, Test, and Evaluation initiatives to advance SDC communication systems, processes and procedures across the program.	20. 99% availability  21. 99% availability  22. 99% availability  23. 99% availability  24. 95% of deliverables submitted on time with no revisions.	20. 99% availability  21. 99% availability  22. 99% availability  23. 99% availability  24. 95% of deliverables submitted on time with no revisions.	20. 99% availability  21. 99% availability  22. 99% availability  23. 99% availability  24. 95% of deliverables submitted on time with no revisions.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**IV. Performance Criteria and Evaluation Summary:**

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
<u>White House Situation Support Staff (WHSSS):</u> 25. Percentage of Classified Network Uptime Availability: Uptime availability of classified networks, phones and peripherals in support of the Situation Room and National Security Council (NSC) 26. Percentage of Continuity of Operations (COOP) and Continuity of Government (COG) Facilities Uptime: Network uptime for Continuity of Operations (COOP) and Continuity of Government (COG) facilities	25. 95%  26. 95%	25. 99%  26. 99%	25. 99%  26. 99%
<u>Defense Information Systems Network (DISN) Enterprise Activities (EA):</u> <u>Defense Satellite Communications:</u> 27. Mission Requests: To support approved mission requests (100% completion) at a targeted level of 99.99%. An “approved mission request” is a Satellite Access Request (SAR).	27. ≥ 99%	27. ≥ 99%	27. ≥ 99%
<u>DoD Enterprise Cloud Computing Ecosystem:</u> 28. Number of JWCC customers with active task orders (Note: the JWCCs vehicle was awarded in December 2022 (FY 2023)	28. N/A	28. 6	28. 12
<u>Joint Staff Support Center (JSSC):</u> 29. Availability: IT Support for over 1,000 Nuclear Decision Conferences and over 600 Worldwide GCCS-J/JOPEs sites. Target is to maintain 99% of global availability of critical sites world-wide and 24x7 monitoring and reporting of GCCS-J and NCCS systems status, and operational impacts.	29. 100%	29. 100%	29. 100%
<u>Field Command and Field Offices (FC/FO):</u> 30. FC/FO review DISA service support plans, Theater Campaign Plans (TCP), and Operational Plans (OPLAN) 31. Assess threat, vulnerability, and risk to the CCMD Theater Critical Assets 32. Assess Command, Control, Computer, Communication, Intelligence, Surveillance and Reconnaissance (C4ISR) readiness, service constraints and delivery. 33. FC/FO participate in U.S./Indo-Pacific/NATO DISA C4ISR interoperability reviews	30. 41  31. 65 32. 14  33. 5	30. 45  31. 69 32. 17  33. 5	30. 50  31. 72 32. 20  33. 6

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**IV. Performance Criteria and Evaluation Summary:**

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
<u>Network Operations (NetOps):</u> 34. Mitigate DISN service interruptions average per month. 35. Block and/or mitigate DISN malicious cyber events average per month. 36. Manage DISN NetOps network assets. 37. C2 Service Telecommunications Service Orders (TSO) and circuit actions.	34. 50,000 35. 380 Million 36. 220 Million 37. 50,000	34. 53,000 35. 400 Million 36. 205 Million 37. 52,000	34. 55,000 35. 420 Million 36. 210 Million 37. 54,000
<u>Standardized Tactical Entry Point (STEP):</u> 39. System availability: Maintain 99.999% system availability for strategic and tactical SATCOM users.	39. 99.999%	39. 99.999%	39. 99.999%
<u>Shared Services Units/Program Executive Offices:</u> 40. Number of DODNET user accounts to validate to ensure DISA employees are licensed legally and accurately	40. 6711	40. 7100	40. 9100
<u>Defense Spectrum Organization (DSO):</u> 41. Deploy at least one new release to DSO data services and analytics per year. 42. Data services availability maintained above 97%. 43. Deliver at least one data product per year. 44. Maintain 97% operational availability of JSIR-O system. 45. Deploy one architectural segment every 12 months with each segment having on average 40 architectural artifacts (views, descriptions, etc.) 46. Engineering services technical analyses	41. 1 42. 99.8% 43. 1 44. N/A 45. 1 46. 462	41. 1 42. 97% 43. 1 44. 97% 45. 1 46. 450	41. 1 42. 97% 43. 1 44. 97% 45. 1 46. 450
<u>Global Command and Control System-Joint (GCCS-J):</u> 47. Number of GCCS-J sustainment releases supported [i.e., fixes, capability sustainment]	47. 9	47. 6	47. 6



**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**IV. Performance Criteria and Evaluation Summary:**

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
<u>Joint Planning and Execution Services (JPES):</u>			
48. JOPES Availability	48. 100%	48. 95%	48. 95%
49. Number of JOPES Releases	49. 1	49. 1	49. 0
50. JCRM Availability	50. 99%	50. 95%	50. 95%
51. Number of JCRM Releases	51. 1	51. 2	51. 3

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**V. Personnel Summary:**

	<u>FY 2022</u>	<u>FY 2023</u>	<u>FY 2024</u>	<u>Change FY 2022/ FY 2023</u>	<u>Change FY 2023/ FY 2024</u>
<b>Active Military End Strength (E/S) (Total)</b>	<b>1,629</b>	<b>1,644</b>	<b>1,645</b>	<b>15</b>	<b>1</b>
Officer	371	387	388	16	1
Enlisted	1,258	1,257	1,257	-1	0
<b>Reserve Drill Strength (E/S) (Total)</b>	<b>15</b>	<b>15</b>	<b>15</b>	<b>0</b>	<b>0</b>
Officer	1	1	1	0	0
Enlisted	14	14	14	0	0
<b>Reservists on Full Time Active Duty (E/S) (Total)</b>	<b>0</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>0</b>
Officer	0	10	10	10	0
<b>Civilian End Strength (Total)</b>	<b>2,600</b>	<b>2,594</b>	<b>2,723</b>	<b>-6</b>	<b>129</b>
U.S. Direct Hire	2,467	2,461	2,590	-6	129
<b>Total Direct Hire</b>	<b>2,467</b>	<b>2,461</b>	<b>2,590</b>	<b>-6</b>	<b>129</b>
Foreign National Indirect Hire	5	5	5	0	0
Reimbursable Civilians	128	128	128	0	0
<b>Active Military Average Strength (A/S) (Total)</b>	<b>1,629</b>	<b>1,644</b>	<b>1,645</b>	<b>15</b>	<b>1</b>
Officer	371	387	388	16	1
Enlisted	1,258	1,257	1,257	-1	0
<b>Reserve Drill Strength (A/S) (Total)</b>	<b>15</b>	<b>15</b>	<b>15</b>	<b>0</b>	<b>0</b>
Officer	1	1	1	0	0
Enlisted	14	14	14	0	0
<b>Reservists on Full Time Active Duty (A/S) (Total)</b>	<b>0</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>0</b>
Officer	0	10	10	10	0

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**V. Personnel Summary: (Cont.)**

	<u>FY 2022</u>	<u>FY 2023</u>	<u>FY 2024</u>	<u>Change FY 2022/ FY 2023</u>	<u>Change FY 2023/ FY 2024</u>
<b>Civilian FTEs (Total)</b>	<b>2,600</b>	<b>2,594</b>	<b>2,723</b>	<b>-6</b>	<b>129</b>
U.S. Direct Hire	2,467	2,461	2,590	-6	129
<b>Total Direct Hire</b>	<b>2,467</b>	<b>2,461</b>	<b>2,590</b>	<b>-6</b>	<b>129</b>
Foreign National Indirect Hire	5	5	5	0	0
Reimbursable Civilians	128	128	128	0	0
<b>Average Annual Civilian Salary (\$ in thousands)</b>	<b>165.8</b>	<b>167.9</b>	<b>174.5</b>	<b>2.1</b>	<b>6.6</b>
<b>Contractor FTEs (Total)</b>	<b>3,849</b>	<b>3,874</b>	<b>3,770</b>	<b>25</b>	<b>-104</b>

**Personnel Summary Explanations:**

**Military end strength (+1)** An increase of +1 Army Officer to support the DISA continued force structure growth.

**FY 2023 - FY 2024 is (+129) FTEs.**

1. An increase of +22 FTEs to sustain the voice only Defense Red Switch Network (DRSN) and develop the follow-on system for conference capability.
2. DISA Internal FTE Rephasing (+83) FTEs: A increase of +83 FTEs primarily reflects an internal rephasing of FTEs. The increase reflects an internal realignment from Non-Cyber to Cyber to support the growth in Non-Cyber missions, as well as, to reflect the proper Average Annual Rate (AAR) for the agency to ensure mission readiness.
3. An Increase of +24 FTEs to support mission to build, operate, monitor, train, and maintain the classified enterprise wide PITC-Secret and PITC-TS network.

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**VI. OP 32 Line Items as Applicable (Dollars in thousands):**

	FY 2022*	Change from FY 2022 to FY 2023		FY 2023	Change from FY 2023 to FY 2024		FY 2024**
		Program	Price Growth		Program Growth	Price Growth	
101 EXEC, GEN'L & SPEC SCHEDULES	409,945	16,931	-12,736	414,140	20,823	17,891	452,854
<b>0199 TOTAL CIVILIAN PERSONNEL COMPENSATION</b>	<b>409,945</b>	<b>16,931</b>	<b>-12,736</b>	<b>414,140</b>	<b>20,823</b>	<b>17,891</b>	<b>452,854</b>
308 TRAVEL OF PERSONS	30,228	635	5,887	36,750	809	-9,769	27,790
<b>0399 TOTAL TRAVEL</b>	<b>30,228</b>	<b>635</b>	<b>5,887</b>	<b>36,750</b>	<b>809</b>	<b>-9,768</b>	<b>27,790</b>
671 DISA DISN SUBSCRIPTION SERVICES (DSS)	54,847	1,766	-32,400	24,213	1,567	219	25,999
672 PRMRF PURCHASES	0	0	31,720	31,720	4,622	-3,767	32,575
677 DISA TELECOMM SVCS - REIMBURSABLE	16,444	0	39,685	56,129	3,648	-2,677	57,100
696 DFAS FINANCIAL OPERATION (OTHER DEFENSE AGENCIES)	9,025	494	4,390	13,909	106	773	14,788
<b>0699 TOTAL OTHER FUND PURCHASES</b>	<b>80,316</b>	<b>2,260</b>	<b>43,395</b>	<b>125,971</b>	<b>9,943</b>	<b>-5,452</b>	<b>130,462</b>
771 COMMERCIAL TRANSPORT	3,273	69	908	4,250	85	30	4,365
<b>0799 TOTAL TRANSPORTATION</b>	<b>3,273</b>	<b>69</b>	<b>908</b>	<b>4,250</b>	<b>85</b>	<b>30</b>	<b>4,365</b>
912 RENTAL PAYMENTS TO GSA (SLUC)	51,912	1,090	-42,352	10,650	234	137	11,021
913 PURCHASED UTILITIES (NON-FUND)	3,785	79	3,697	7,561	166	-151	7,576
914 PURCHASED COMMUNICATIONS (NON-FUND)	43,244	908	-9,667	34,485	759	2,363	37,607
915 RENTS (NON-GSA)	49	1	81	131	3	6	140
917 POSTAL SERVICES (U.S.P.S)	3	0	174	177	4	-4	177
920 SUPPLIES & MATERIALS (NON-FUND)	3,516	74	5,186	8,776	193	36	9,005
921 PRINTING & REPRODUCTION	4,541	95	-4,634	2	0		2
922 EQUIPMENT MAINTENANCE BY CONTRACT	1,182,604	24,835	136,933	1,344,372	29,576	195,973	1,569,921
923 FACILITIES SUST, REST, & MOD BY CONTRACT	18,834	396	-2,190	17,040	375	2,978	20,393
925 EQUIPMENT PURCHASES (NON-FUND)	104,294	2,190	-63,517	42,967	945	34,934	78,846
932 MGT PROF SUPPORT SVCS	0	0	1,245	1,245	27	165	1,437
933 STUDIES, ANALYSIS & EVAL	2,721	57	-697	2,081	46	-1,158	969
934 ENGINEERING & TECH SVCS	48,480	1,018	-47,722	1,776	39	73	1,888
937 LOCALLY PURCHASED FUEL (NON-FUND)	89	-7	-82	0	0	0	0

**Defense Information Systems Agency  
Operation and Maintenance, Defense-Wide  
Fiscal Year (FY) 2024 Budget Estimates**

**VI. OP 32 Line Items as Applicable (Dollars in thousands):**

	FY 2022 <u>Program</u>	<u>Change from FY 2022 to FY 2023</u>		FY 2023 <u>Program</u>	<u>Change from FY 2023 to FY 2024</u>		FY 2024 <u>Program</u>
		<u>Price Growth</u>	<u>Program Growth</u>		<u>Price Growth</u>	<u>Program Growth</u>	
957 OTHER COSTS (LAND AND STRUCTURES)	923	19	-942	0	0	0	0
987 OTHER INTRA-GOVT PURCH	489	10	101,921	102,420	2,253	11,084	115,757
988 GRANTS	0	0	33	33	1	-34	0
989 OTHER SERVICES	23,407	492	72,566	96,465	2,122	-1,099	97,488
990 IT CONTRACT SUPPORT SERVICES	32,183	676	-32,859	0	0	0	0
<b>0999 TOTAL OTHER PURCHASES</b>	<b>1,521,074</b>	<b>31,933</b>	<b>117,174</b>	<b>1,670,181</b>	<b>36,743</b>	<b>245,303</b>	<b>1,952,227</b>
<b>9999 GRAND TOTAL</b>	<b>2,044,836</b>	<b>51,828</b>	<b>154,628</b>	<b>2,251,292</b>	<b>68,403</b>	<b>248,004</b>	<b>2,567,698</b>