

Fiscal Year 2027 Budget Estimates

Defense Information Systems Agency



April 2026

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

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

	<u>FY 2025 Actuals</u>	<u>Price Change</u>	<u>Program Change</u>	<u>FY 2026 Enacted</u>	<u>Price Change</u>	<u>Program Change</u>	<u>FY 2027 Request</u>
DISA	2,635,636	45,639	274,290	2,955,565	51,638	866,019	3,873,222

I. Description of Operations Financed:

The Defense Information Systems Agency (DISA) is a critical combat support agency that delivers, operates, and assures the foundational Command and Control, information sharing capabilities, and global enterprise information infrastructure essential for joint warfighters, national-level leaders, and coalition partners across the full spectrum of operations.

The DISA Next Strategy directly drives combat support priorities and initiatives, ensuring the delivery of essential capacity and capability for warfighting information systems. Through planning, engineering, acquisition, testing, fielding, operation, and assurance, DISA develops and maintains robust information-sharing capabilities, Command and Control solutions, and a global enterprise infrastructure supporting the Department of War (DoW) and national leadership.

DISA drives innovation and fosters collaboration to align capabilities with evolving threats. The agency is integral to achieving the Secretary of War's priorities: rebuilding the military, reestablishing deterrence, and defending the homeland. By embodying core principles of readiness, campaigning, continuous modernization, and establishing lethality, DISA ensures the military remains agile and adaptable, capable of rapidly incorporating new technologies and tactics to counter evolving threats.

In support of the President's 2025 National Security Strategy, DISA continuously modernizes its network infrastructure and cyber defenses to outpace evolving threats and drive technological advancements. This ensures a resilient, secure, and scalable network for forces at home and forward-deployed Combatant Commands (CCMDs). These efforts are crucial to maximizing resilience against foreign adversaries and enabling seamless interoperability between the Department of War and its allies.

Serving the President, Vice President, Secretary of War, Joint Chiefs of Staff, CCMDs, and other DoW Components, DISA provides essential networks, computing infrastructure, and enterprise services. These resources enable critical information sharing and decision-making for the nation's warfighters and their support elements, directly contributing to national defense. Committed to advancing technology, DISA strengthens the security and resilience of networks and systems, thereby enhancing current and future U.S. military advantages over adversaries. Key priority areas include Cybersecurity, National Leadership Command Capability, and White House support.

Four strategic imperatives guide DISA's efforts:

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Strategic Imperative #1: Operate and Secure the DISA Portion of the DoW Information Network

This imperative demands fortifying foundational infrastructure, continuously innovating processes, dedicating critical resources, and deploying relevant, modern enterprise and business tools. A resilient and redundant Defense Information Systems Network (DISN) backbone is essential to ensure robust data transport security across the DoW Information Network.

Strategic Imperative #2: Support Strategic Command, Control, and Communications

DISA's critical function is to develop, provision, and operate secure Command, Control, and Communications solutions. Key goals include fully operationalizing cloud capabilities, building an accessible hybrid cloud environment, and strengthening data management standards. These innovations will empower warfighters with the scope and scale of data access needed for modern combat operations, ensuring agility and adaptability against emerging threats.

Strategic Imperative #3: Optimize the Network

Optimizing the DoW Information Network encompasses both enhancing security and improving adaptability. This means innovating the network's infrastructure to instill confidence in its resilience while ensuring a seamless user experience and actively minimizing technical debt. Achieving an unconstrained DoW Information Network and consolidating efforts across Defense Agencies and Field Activities and CCMDs are pivotal goals guiding this imperative.

Strategic Imperative #4: Operationalize Data

Leveraging data to empower warfighters with a strategic advantage over adversaries is paramount to maintaining competitive superiority. This requires aligning culture, conduct, and capabilities to drive innovation in data operationalization. Modernizing the coordination capabilities of the National Leadership Command Capability and enhancing joint warfighting tools will significantly strengthen the collaborative process of putting data into action.

DISA aligns its program resource structure across six mission areas. These mission areas reflect the DoW's national defense priorities and represent DISA's focus on executing its lines of operations:

Transition to Data-Centric Environment: Create and strengthen a trusted network environment to facilitate seamless DoW information sharing by making data continuously available. Cultivate and rapidly integrate emerging technologies into the military's arsenal to maintain a decisive technological edge over adversaries.

Eliminate Bandwidth Constraints: Build and sustain a resilient DoW Information Network transport infrastructure that eliminates bandwidth constraints and rapidly surges to meet demands, whenever and wherever needed.

DoW Information Network Operations and Defense: Operate, protect, defend, and sustain the enterprise infrastructure and information sharing services, enabling critical Command and Control. Support CCMDs by providing advanced cybersecurity and network operations to the edge of conflict.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Exploit the DoW Information Network for Improved Decision Making: Build DoW enterprise-wide capabilities for communities of interest, such as command and control and combat support, that leverage the DoW Information Network for improved decision-making. This enables enhanced collaboration, joint military exercises, intelligence sharing, and strategic planning for deterrence.

Deliver Capabilities Effectively/Efficiently: Deliver capabilities, based on established requirements, more effectively, economically, and efficiently than currently achieved.

Special Mission Area: Execute special missions to provide essential communications support required by the President, including day-to-day management, fielding, operation, and maintenance of critical communications and information technology.

DISA continues to use the Cost Allocation Model to assign shared services costs to products and services. The Cost Allocation Model identifies the total cost of a program and avoids unintended subsidies to the Defense Working Capital Fund), provides visibility into the cost and consumption of shared services, and identifies efficiencies.

Mission Area: Transition to Data-Centric Environment (FY 2027: \$526,607 thousand)

1. DoW Information Network Engineering Services - (FY 2027: \$179,363 thousand): DISA ensures the performance, cost-effectiveness, and interoperability of the DoW Information Network enterprise by applying technical architecture, integration engineering, updated interface standards, and modeling and simulation services. This initiative also maintains critical engineering standards across the DoW, Services, and Agencies. DISA continually enhances its technical engineering capabilities and strives to update essential Command and Control standards every two years. These advancements are crucial for rapidly integrating emerging technologies into the military's arsenal, thereby supporting national defense priorities and maintaining a technological edge over adversaries.

Ongoing DoW Information Network Engineering Services_efforts supported include:

- Promoting centralized technology policy, standards, and leadership through extensive technology outreach, including weekly Technical Exchange Meetings with the DoW Chief Information Officer, federal agencies, and industry. These Technical Exchange Meetings identify best practices, material solutions, mature capabilities, and enterprise services.
- Conducting security engineering and product accreditation within the Technology Analysis Center lab environment. The Technology Analysis Center lab provides flexible, rapidly reconfigurable environments for real-time or near real-time assessment of emerging technologies, accelerating the delivery of leading-edge capabilities to warfighters and mission partners.
- Providing seamless engineering and technical support for technology solutions as they transition to operations and maintenance.
- Delivering cutting-edge network monitoring for Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet). This includes maintaining network sensors and developing advanced algorithms to interpret sensor data.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

- Implementing a comprehensive SIPRNet Endpoint Management solution to enhance security, enabling the DoW to monitor connected devices and uniformly apply security settings across the network.

Modeling and simulation services provide insightful analyses that inform DoW infrastructure services and applications. These services ensure capabilities are planned, implemented, and assessed cost-efficiently to meet performance objectives. They offer predictive analysis, systems engineering, and End-to-End analytical assessments that guide design and investment recommendations. Concurrently, integration engineering confirms that all capabilities are seamlessly integrated to collectively meet warfighter mission requirements. These combined capabilities are crucial for adapting boundary defenses to changing conditions. Boundary defenses must constantly evolve with traffic demands and new solutions like commercial cloud services, thereby strengthening continuous warfighter readiness.

2. Data-Centric Enterprise Services - (FY 2027: \$160,123 thousand): DISA, through Data-Centric Enterprise Services, delivers a comprehensive suite of enterprise collaboration services. These services are vital for an agile and adaptable warfighter support network and directly empower Warfighters, intelligence personnel, and other enterprise users across both SIPRNet and NIPRNet. This strategic alignment with national defense priorities enhances information sharing and operational effectiveness.

The Data-Centric Enterprise Services collaboration portfolio provides:

- Collaborative Connectivity: Enabling over two million authorized DoW users to seamlessly collaborate across CCMDs, Services, the Joint Staff, and various Agencies via web-accessible tools.
- Secure & Resilient Infrastructure: A robust and flexible foundation for secure information sharing, critical for mission success.
- Decoupled Information Exchange: An enterprise messaging service that allows producers to publish perishable and non-perishable data without specifying recipients, while consumers subscribe to mission-critical information, enhancing efficiency and relevance.
- Flexible Data Access: Secure access to web and application content, warfighter intelligence, and critical data, with the flexibility to integrate services as needed.
- Cloud-Enabled Modernization: Supports application rationalization by prioritizing legacy systems for modernization and facilitating their secure transition to commercial and DoW on-premises cloud environments.
- SIPRNet Modernization: Crucial support for SIPRNet modernization initiatives, including department-wide upgrades to Microsoft 365 (M365) Impact Level 6 licenses.

The Defense Enterprise Office Solution provides unified communication, collaboration, and productivity services. It delivers a secure, cost-efficient, and accessible platform through the Microsoft 365 suite across both unclassified (DOW365-J) Impact level 5 Tenant and classified (DOW365-SEC) Impact level 6 networks. By optimizing support for military operations, streamlining information access, strengthening cybersecurity, and simplifying the DoW's Information Technology (IT) footprint, Defense Enterprise Office Solution transcends legacy office productivity and collaboration tools. By offering a unified suite of tools and services, Defense Enterprise Office Solution aims to enhance mission effectiveness across the DoW, promoting collaboration and efficiency across various agencies and CCMDs.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Complementing Defense Enterprise Office Solution, Enterprise Messaging enables users to communicate across applications on both NIPRNet and SIPRNet. Leveraging a publish-subscribe model, Enterprise Messaging dramatically reduces the complexity of peer-to-peer integrations. Its modernization has delivered a cloud-based transport solution built on open and lightweight protocols, promoting easier and more flexible enterprise-wide integration.

3. DoW Enterprise Cloud Computing Ecosystem - (FY 2027: \$187,121 thousand): DISA delivers industry-leading cloud hosting and computing capabilities to the DoW, the Joint Force, and ultimately, the warfighter. These advanced cloud capabilities enable DoW personnel and warfighters to securely and efficiently access mission-critical data from any location. Through its DoW Enterprise Cloud Computing Ecosystem program, DISA drives readiness and innovation by providing best-value hybrid cloud offerings. These enhancements in cloud computing fortify a critical technological edge over adversaries. Current key offerings include the Joint Warfighting Cloud Capability and Cloud Accelerators.

The Joint Warfighting Cloud Capability is the portfolio's primary offering. This multi-vendor, enterprise-wide acquisition vehicle empowers the DoW to directly procure commercial cloud services from leading Cloud Service Providers. The Joint Warfighting Cloud Capability delivers a first-of-its-kind capability, encompassing the needs of the entire enterprise across all classification levels, including dedicated top-secret cloud environments. As the first enterprise contract vehicle available DoW-wide, the Joint Warfighting Cloud Capability extends the power of commercial cloud directly to the warfighter. This capability is key for critical initiatives such as Combined Joint All-Domain Command and Control and Zero Trust, significantly enhancing the Department's operational effectiveness. Furthermore, once a DoW customer selects a commercial cloud option, the Joint Warfighting Cloud Capability provides integrated layers of monitoring and cybersecurity.

Cloud Accelerators equip mission partners with innovative tools designed to streamline cloud adoption. These products simplify and expedite the ordering, provisioning, onboarding, securing, and management of cloud services, ensuring maximum efficiency and cost-effectiveness in procurement. Current capabilities include:

- DoW Cloud Infrastructure as Code: Leverages automation and accredited baselines to rapidly build and deploy secure cloud environments, significantly reducing setup times for faster cloud adoption.
- Account Tracking and Automation Tool: A cloud provisioning tool that automates the creation of accounts across multiple cloud vendors and classification levels, while tracking expenditures against task orders.
- DISA Acquisition Package Preparation System: A web-based interview tool that guides mission owners in developing comprehensive acquisition packages, streamlining the DoW acquisition process and expediting Joint Warfighting Cloud Capability task order awards.
- Joint Operational Edge: Delivers commercial Infrastructure as a Service and Platform as a Service to Mission Partners via on-premises, interconnected edge computing platforms installed at DoW locations. In FY 2027, DISA is adding artificial intelligence acceleration hardware to existing Joint Operational Edge sites, putting powerful artificial intelligence tools directly in the hands of tactical mission partners.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

- **Joint Unmanaged Landing Zones:** In FY 2027, DISA is installing landing zones, which will function as accredited, pre-approved security boundaries with corresponding network gateways on SIPRNet, for all four Joint Warfighting Cloud Capability providers.

DISA is expanding cloud computing capabilities in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. Cloud computing contributes to Mission Network as a Service by providing a secure and high-powered cloud environment to access applications and perform complex analysis using artificial intelligence. Cloud computing expansion and enhancement directly support the Secretary of War's priorities by rebuilding the overseas digital infrastructure, restoring readiness by giving forward troops faster access to data and artificial intelligence, and reestablishing deterrence by deploying leading technology to the tactical edge.

Mission Area: Eliminate Bandwidth Constraints (FY 2027: \$967,085 thousand)

1. **Defense Information Systems Network Enterprise Activities - (FY 2027: \$682,928 thousand):** The Defense Information Systems Network is DoW's consolidated, worldwide telecommunications infrastructure. It provides critical, end-to-end Command, Control, Communications, Computers, and Intelligence information transport for warfighters and Combatant Commanders. Seamlessly spanning terrestrial to space and strategic to tactical domains, the Defense Information Systems Network delivers the interoperable connectivity essential for planning, implementing, and supporting all operational missions, anytime, anywhere. Continuous enhancement of the Defense Information Systems Network is crucial to providing warfighters with the superior network resources needed to maintain strategic advantage against evolving adversarial threats. In FY 2027, DISA is refreshing the Defense Information Systems Network's Internet Protocol and Optical capabilities. By operationalizing a state-of-the-art, all-Internal Protocol and optical core, the Defense Information Systems Network will be faster and more secure with embedded in-flight encryption and capable of handling operations at multiple classification levels.

Major Defense Information Systems Network capabilities include the following:

Airborne Intelligence, Surveillance & Reconnaissance: Airborne Intelligence, Surveillance & Reconnaissance supports Combatant Commanders, Services, and Agencies by collecting, analyzing, and disseminating critical sensor data to globally dispersed strategic, operational, and tactical customers. This timely and assured delivery of fused intelligence is crucial for achieving information superiority, directly supporting Counterterrorism, Theater Campaign Plans, and Contingency Operations. Airborne Intelligence, Surveillance & Reconnaissance funding sustains the vital capabilities required for end-to-end transport and tailored dissemination of this data, ensuring it reaches DoW and Mission Partners precisely when and where it's needed.

Resilient Ground Infrastructure: Airborne Intelligence, Surveillance & Reconnaissance Ground Entry Points deliver sensor data from unmanned and manned airborne platforms directly to deployed warfighters, enhancing their effectiveness and lethality. The ground infrastructure requires robust, redundant ground entry points across diverse frequency bands and sites to ensure continuous support for U.S. Warfighting forces, even if individual ground entry points become unavailable.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

The criticality of this infrastructure prompted the DoW CIO to commission the Gateway Optimization and Resiliency Study. Completed and accepted in July 2022, the Gateway Optimization and Resiliency Study comprehensively assessed the resiliency of the entire DoW satellite communication Enterprise's ground infrastructure. In response to Gateway Optimization and Resiliency, Airborne Intelligence, Surveillance & Reconnaissance Resilient Ground Infrastructure will strengthen the ground entry points, guaranteeing the assured delivery of critical Intelligence, Surveillance & Reconnaissance data to globally dispersed CCMDs and engaged forces. This directly improves their ability to negate adversary maneuver and achieve decisive victory by increasing capacity, resiliency, and geographic diversity. Reliable communications, intelligence access, and battlespace awareness are paramount to the Secretary of War's priorities of readiness and lethality. O&M covers essential equipment operations, maintenance, and sustainment.

Defense Red Switch Network: The Defense Red Switched Network provides a highly secure, multi-level SECRET to Top Secret/Sensitive Compartmented Information voice and conferencing capability. It enables rapid, ad-hoc communications for the President, Secretary of War, Services, CCMDs, their subordinate organizations (military and civilian), and coalition allies. The Defense Red Switched Network is essential for meeting Nuclear Command and Control Communications requirements and for supporting emergency conference protocols. Sustainment funding is critical for the continued operation and reliability of this vital network

Classified Voice and Video: DISA has developed the Classified Voice and Video capability, an Internet Protocol-based capability enabling secure communication across multiple classification levels on a single platform. Classified Voice and Video will be in sustainment in FY 2027: DISA will sustain the initial capability, including a pre-production environment, three geographically dispersed sites in Region 1 (East), an Initial Operating Capability Network Operations Center and an Initial Operating Capability Security Operations Center (SOC). DISA will deploy Classified Voice and Video to three additional sites to expand the capability to Region 2 (Central). Classified Voice and Video is critical for supporting the nation's Nuclear Command Control Communications system, which demands resilient command and control of U.S. nuclear forces under all circumstances, including during and following a nuclear or non-nuclear attack. Resilient Nuclear Command Control Communications capabilities are fundamental for nuclear operations mission assurance. As a key modernization program, Classified Voice and Video enhances DoW secure conferencing, meeting National and Military leadership's essential Command and Control and Decision-Making functions, and addressing evolving technology and security requirements.

Enhanced Pentagon Capability/Survivable Emergency Conferencing Network: The Enhanced Pentagon Capability/Survivable Emergency Conferencing Network delivers vital, highly classified communication for senior national and military leadership. It strictly adheres to the Nuclear Technical Performance Criteria, guaranteeing continuous, optimal performance that is critical for strategic command and control.

DoW Mobility: The DoW Mobility Program provides comprehensive, secure mobile communications, enabling both unclassified and classified access through the following critical service platforms:

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

- **DoW Mobility Unclassified Capability:** Delivers unclassified mobile device access to DoW Information Network and commercial information services for Senior Leaders, Defense Agencies and Field Activities, and CCMDs. DISA has begun migrating new devices to the Microsoft InTune mobile security capability and will expand to devices across all Defense Agencies and Field Activities. InTune promotes rapid delivery and utilization of secure mobile capability, leveraging commercial mobile technologies to enable an agile deployment environment for new and innovative applications to support evolving Warfighter requirements.
- **DoW Mobility Classified Capabilities Secret:** Enables government-owned mobile devices to access Classified Secret DoW Information Network telephony and information services.
- **DoW Mobility Classified Capabilities Top Secret:** Provides mobile device access to Top Secret Collateral DoW Information Network telephony services.

Funding for the Mobility Program sustains essential gateway and infrastructure support, along with critical program management.

Interoperability and Internet Protocol Enabling: The DoW Network Information Center is central to the planning, management, and sustainment of Domain Name System capabilities for the global Internet, the classified SECRET and unclassified CUI Defense Information Systems Network. DISA's role extends to facilitating the delivery of voice, video, and data services across an interoperable, secure, and highly available Internet Protocol (IP) network infrastructure.

DISA's IP Enabling function provides comprehensive management and registration of all DoW IP number resources, serving as the recognized DoW agent for IP number management by external internet governance organizations. It also offers "Who Is" query capabilities for IP number registrations and .MIL domain information, directly benefiting DoW and intelligence community organizations.

To enhance these capabilities, DISA is actively converting to a global converged infrastructure through IP version 6. This enables superior fault isolation and dynamic routing of network traffic, ensuring enhanced service delivery and preventing critical service interruptions for the warfighter and end user.

DISN Resiliency: Defense Information Systems Network Resiliency enhances the resiliency and reliability of the Defense Information Systems Network Core infrastructure and supports CCMDs warfighting Command, Control, Communications, Computers, and Intelligence capabilities by procuring infrastructure to eliminate vulnerabilities that would have debilitating impacts on these capabilities. Funding supports capabilities associated with the Global Defense Information Systems Network Resiliency Program.

Senior National Leadership Communications - Communications with Other Nations: Senior National Leadership Communications - Communications with Other Nations provides secure voice, video, and data communications between U.S. senior leaders and their international counterparts. These critical links are essential for fostering cooperation, de-escalating tensions, and advancing nuclear reduction initiatives. Key components sustained by this funding include:

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

- **Washington-Moscow Direct Communications Link:** A highly secure, dedicated communication pathway (terrestrial and satellite) connecting senior Russian leadership directly with the President of the United States (POTUS), SECWAR, Chairman of the Joint Chiefs of Staff (CJCS), and the State Department's Nuclear Risk Reduction Center for critical data, voice, and video exchanges.
- **Defense Telephone Link:** Facilitates secure voice and video interactions between U.S. Senior Leaders (e.g., SECWAR, CJCS, CCMDs, Policy Directors) and their counterparts in approximately 40 allied and partner nations.
- **Equivalent Value Exchange Memorandum of Understanding:** Governs and sustains robust, long-standing communications interoperability and strategic data/resource sharing between the DoW and its Five Eyes partners (United States, United Kingdom, Canada, Australia, New Zealand). This Memorandum of Understanding also ensures continuous data exchange with the Israel Defense Forces across information technology infrastructure, data, and voice platforms.

Proliferated Low Earth Orbit: A network of satellites that creates a reliable communications network for the warfighter. Proliferated Low Earth Orbit securely connects DoW users of Proliferated Low Earth Orbit with Defense Information Systems Network Core Infrastructure services. The Proliferated Low Earth Orbit network is a layer of satellites that allow ground stations and satellites to connect. The network consists of many redundant and overlapping smaller satellites, eliminating the risk of having a network with a single point of failure.

The Proliferated Low Earth Orbit is crucial for DISA operations because it provides lower latencies in transmissions between users, provides a transmission platform with multiple redundancies in the case of satellite failure or foreign adversary action, and is less expensive to insert in the operating environment.

DISA is deploying five Proliferated Low Earth Orbit/Software-Defined Wide Area Network enabled deployable Defense Information Systems Network nodes. The Proliferated Low Earth Orbit Defense Information Systems Network Software-Defined Wide Area Network nodes provide resilient connectivity to classified and unclassified voice, video, and data services, allowing the Warfighter to connect to the Defense Information Systems Network anywhere in the world. They are portable and can be shipped to emerging global hotspots, enabling the warfighter to connect to the Defense Information Systems Network before permanent infrastructure is available reliably.

Critical Time Dissemination: Success in the modern, contested battlespace depends on coordinated and reliable timing across all DoW mission systems. The critical time dissemination program delivers a critical capability by distributing precise, Coordinated Universal Time (UTC)-traceable Timing & Frequency signals across the DoW Information Network. This supports the full spectrum of DoW missions, from tactical to enterprise, at sites throughout the Continental United States and Outside the Continental United States, addressing the Warfighter's growing need for robust and precise synchronization. In partnership with other DoW organizations, DISA has deployed 46 major Defense Regional Clock and 30 Timing and Synchronization System Capability suites globally. Ongoing efforts are focused on enhancing the program's Monitoring and Control capabilities and establishing a resilient infrastructure. This robust timing infrastructure directly supports the Secretary of War's priority of Reestablishing Deterrence by ensuring our defense mechanisms are prepared to protect the homeland. DISA is developing Critical Time Dissemination capabilities in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. Critical Time Dissemination contributes to Mission Network as a Service by proving the

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Combined Joint Force with precision timing when using Defense Information Systems Network and Command and Control services to conduct sensitive targeting operations.

2. Defense Spectrum Organization - (FY 2027: \$56,412 thousand): Access to the Electromagnetic Spectrum is essential for modern military operations and national security. DISA delivers Electromagnetic Spectrum Operations capabilities through specialized software, engineering, and analytical services. These capabilities enable U.S. and coalition forces to operate effectively, mitigating harmful Electromagnetic Spectrum interference and securing decisive advantages in contested and congested electromagnetic spectrum environments. As the primary provider for many of the DoW's Electromagnetic Spectrum Operations requirements, DISA delivers seamless spectrum access for data links and decision-making across all DoW levels.

DISA develops critical spectrum capabilities through programs like Electromagnetic Battle Management-Joint, the DoW's Joint Electromagnetic Spectrum Command and Control system vital for Combined Joint All-Domain Command and Control. The Global Electromagnetic Spectrum Information System provides enterprise-wide tools for spectrum supportability, host nation coordination, and maintains the authoritative Joint Spectrum Data Repository. Additionally, DISA facilitates Dynamic Spectrum Sharing with interagency partners.

In FY 2027, DISA is moving its spectrum capabilities to a common platform – Maven Smart Systems so they are easily accessible on a secure, modern, cloud-based platform.

DISA's spectrum mission is integral to information operations, electronic warfare, and other Joint Staff initiatives. Specifically, DISA:

- Enhances Joint Electromagnetic Spectrum Battle Management for CCMDs and Joint Task Forces, improving Electromagnetic Spectrum Situational Awareness and Command and Control.
 - Delivers Comprehensive Situational Awareness with data services and analytics, enabling timely decision-making within the Combined Joint All-Domain Command and Control framework.
 - Improves DoW spectrum data quality to enable Artificial Intelligence/Machine Learning applications and mitigate interference.
 - Manages Interference Resolution through the Joint Spectrum Interference Resolution program, providing engineering services for critical national defense systems.
 - Guides Future Capability Development by creating architectural products that ensure interoperability and support national spectrum sharing initiatives.
3. Defense Information Systems Network Infrastructure Services - (FY 2027: \$27,927 thousand): These resources fund DISA's consumption of critical DISN enterprise services from the DISA Defense Working Capital Fund. The Defense Information Systems Network provides essential infrastructure services for warfighter IT functionality, enhancing mission readiness with secure voice, video, and data services. These secure voice and video capabilities operate across classified and unclassified networks, integrating unique military security requirements into

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

commercially competitive solutions. The Defense Information Systems Network's capabilities are crucial for delivering continuous, reliable, and secure voice, video, and data services at mission speed.

4. DoW Teleport Program - (FY 2027: \$87,960 thousand): The DoW satellite communications ground infrastructure provides crucial connection points for deployed U.S. Warfighting forces to access the DoW Information Network. The DoW Information Network access enables warfighters to coordinate maneuver and logistics, and to tap into the extensive information held by U.S. military and intelligence agencies. Without this critical information, deployed warfighters would face increased uncertainty regarding adversarial forces and reduced operational effectiveness.

The DoW Teleport program acquires and modernizes the ground infrastructure for DoW satellite communications. This infrastructure connects deployed U.S. Warfighting forces to the DoW Information Network's fixed elements, granting them access to critical DISN services such as SIPRNet, NIPRNet, the Defense Red Switch Network, the Defense Switched Network, Video Teleconference, and other classified systems. Teleport thus enables U.S. Warfighters to leverage the DoW Information Network for communication across theaters, regions, and globally.

The DoW Teleport program is an Acquisition Category III combined program, which acquires and modernizes satellite communications capabilities, providing diverse communication interfaces between Defense Information Systems Network terrestrial and tactical satellite communications assets through a single point of presence. It provides deployed warfighters with multiband, multimedia, and worldwide reach-back capabilities to Defense Information Systems Network services, ensuring interoperability between multiple satellite communications systems and deployed warfighter tactical networks. These Joint satellite communications Teleports serve as a vital dissemination interface between deployed warfighters and the terrestrial DoW Information Network, connecting them with U.S. installations and depots and providing access to Defense Information Systems Network services and DoW Information Network information.

The Teleport Resilient Ground Infrastructure initiative is increasing the capacity, resilience, and geographic diversity of DISA-managed satellite communications ground infrastructure to support deployed Warfighting forces. Reliable and resilient communications, access to intelligence data, and battlespace awareness are critical for supporting the Secretary of War's priorities of maintaining readiness and enhancing lethality.

The DISA satellite communications Joint Management Tool, formerly known as satellite communications Ordering, Management & Situational Awareness Tools, provides a common operating environment for the DoW's Enterprise Satellite Communications Management and Control. It also forms the foundation of the U.S. Space Force's satellite communications vision and Force Design, enabling the rapid integration of military, commercial, and partnered satellite communications network services through automated resource allocation and mitigation of adversarial spectrum activity. Joint Management Tool is also one of the most critical elements of Combined Joint All-Domain Command and Control technical modernization. It consolidates multiple legacy offerings to streamline the processes for ordering and providing satellite resources to the warfighter, thereby ensuring mission-critical satellite communications capabilities remain available in an era of great power competition. In the United States Indo-Pacific Combatant Command theater alone, approximately 920 hours per year were spent correcting satellite communications resource allocation requests prior to JMT. The Joint Management Tool centralizes and automates fragmented, time-intensive processes for requesting, managing, and allocating mission-critical satellite communications bandwidth. The Joint management Tool

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

will be in sustainment in FY 2027; funding will sustain and enhance Joint management Tool to meet ongoing DoW satellite resource, cybersecurity, and data management requirements.

5. DoDNet /Combatant Command Network Optimization / 4th Estate Network Optimization - (FY2027: \$111,858 thousand): DISA is designated as the single service provider of common-use IT for Defense Agencies and Field Activities and is consolidating commodity IT local area networks and service desks across 16 Defense Agencies and Field Activities. The goal is to migrate disparate organizational networks to a single DoDNet. Post-migration, each DAFA will use DoDNet as its primary network in a common IT environment. This migration to DoDNet facilitates cost savings by adopting enterprise IT delivery models.

Migration to DoDNet promotes Zero Trust compliance, as DAFAs will gain Zero Trust capabilities via DISA's Thunderdome program. DISA expects ten DAFAs to be fully operational on DoDNet in FY 2027 with the remaining six DAFAs completing network infrastructure migration during FY 2027. Adopting the single-service-provider framework will significantly strengthen DAFAs' cybersecurity, drive uniform adoption of IT enterprise services, reduce duplicative IT, and simplify network administration, resulting in an advanced, safeguarded, and consolidated network with integrated, state-of-the-art Zero Trust capabilities.

Beginning in FY 2027, DISA will migrate 11 CCMDs from their legacy networks into a single network for their core IT that leverages DoDNet's infrastructure: Combatant Command Network Optimization. Combatant Command Network Optimization implements DoW's Zero Trust architecture at the operational level, ensuring that each CCMD gains immediate access to advanced cybersecurity protection through DISA's Thunderdome program. By eliminating 11 separate network perimeters and standardizing security protocols, DISA can concentrate defensive cyber operations, deploy patches and upgrades instantaneously across the enterprise, and achieve a level of network visibility impossible to attain with fragmented systems.

DISA is developing Combatant Command Network Optimization in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. Combatant Command Network Optimization contributes to Mission Network as a Service by providing the network infrastructure the Combined Joint Force will use to access Defense Information Systems Network and Command and Control services.

Mission Area: DoW Information Network Operations and Defense (FY 2027: \$220,071 thousand)

1. Field Commands and Field Offices - (FY 2027: \$125,426 thousand): The DISA FC/FO ensures the DoW Information Network's voice, video, and data services align with the Joint Cyber Warfighting Architecture and fulfill global warfighter needs across all conflict phases. These FC/FOs support Combatant Command staff and facilitate the integration of DISA services within Joint All Domain Operations Operational Plans.

The Field Commands and Field Offices assist the DoW in deterring aggression and prevailing in conflict when necessary, prioritizing pacing threats in regionally challenged areas. Sustaining a resilient Joint Force and defense ecosystem demands ongoing IT services, facility/space

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

accommodations, and programmatic operational support worldwide at eleven CCMDs and National Military Command Center HQ locations. These Field Commands and Field Offices also align effective, on-site strategic Command and Control and situational awareness among the CCMDs, Military Departments, Defense Agencies and Field Activities, and deployed forces, supporting National Security by:

- Preparing and publishing DISA support plans for all Combatant Command Theater Campaign Plans, global campaign plans, and contingency plans.
- Reviewing and recommending DISA service improvements to more than 50 Operational Plans annually.
- Providing customer service support and requirements advocacy to all stakeholders subscribing, or planning to subscribe, to DISA's existing or emerging information products and services.
- Enabling effective coordination and information exchange in support of services, policy, planning, and new capabilities.
- Sustaining Combined Joint All-Domain Command and Control/DoW Information Network services by assigning DISA Field Commands and Field Offices_employee specialists worldwide to each CCMDs HQ facility.
- Developing solutions for specific warfighting capability gap requirements identified in the Integrated Priority Lists for the Chairman of the Joint Chiefs of Staff.
- Defending the DoW Information Network by assuring system and network availability, information delivery, and information protection across strategic, operational, and tactical boundaries in support of the DoW, CCMDs, Military Departments, Defense Agencies and Field Activities, and the Joint Staff.
- Actively participating in Joint and coalition exercises.
- Conducting assessments of threat, hazards, vulnerability, and risk to DoW-owned Defense Critical Infrastructure and the inter/intra-dependencies required to execute critical DoW missions without fail, in accordance with DoW Directive 3020.40, DoW 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. This work occurs via the Critical Infrastructure Program, which identifies, labels, and prioritizes the DoW Information Network sector and DISA assets.
- Developing Continuity of Operations plans and exercises to ensure essential functions and operations continue throughout various threats, contingency operations, and humanitarian disasters.

Additional missions include:

- Working with United States Indo-Pacific Combatant Command coalition partners and North Atlantic Treaty Organization (NATO) Field Offices to ensure U.S./Indo-Pacific/NATO partnership consideration in all planning and design efforts to facilitate C4ISR interoperability. The program is prepared to deter aggression and overcome conflict in the Indo-Pacific.
- Providing support to Indo-Pacific coalition partners and NATO Ministry of Communications and Information Technology for transforming Information and Communication Technology in support of business stabilization, while encouraging strategic economic growth in other areas of operational responsibility.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

2. Network (DoW Information Network) Operations - (FY 2027: \$64,324 thousand): DISA ensures that the DoW Information Network (spanning voice, video, and data services) capabilities, access points, and boundary protections meet critical DoW mission requirements. DISA leads technical refresh, configuration control, and sustainment to improve service delivery to the warfighter, achieving end-to-end interoperability and increasing competitive strength over adversaries.

DISA provides continuous DoW Information Network operational service delivery in 42 countries at 3,800 locations worldwide, serving CCMDs, Military Departments, Defense Agencies and Field Activities, and Joint Staff centers across U.S. global military operations. It delivers continuous situational awareness, ensures DoW Information Network resilience, and conducts intelligence activities to identify and assess network threats. It also develops threat assessments, drawing on intelligence from the Defense Intelligence Enterprise, to inform decision-making for both fielded and developing systems and capabilities. By fulfilling these duties, it mitigates service interruptions, anticipates threats, develops alternate configurations, and provides enhanced mission support for no-fail services.

DISA also supports the United States Cyber Command (USCYBERCOM) mission to provide secure, interoperable, and reliable operations across the DoW Information Network within the JCWA. DISA's primary tasks in this capacity are:

- Operating and defending the DoW Information Network, enabling DoW Enterprise services support to the USCYBERCOM internal and external Cyberspace Operations, DoW Cyber Operations Forces, Defensive Cyber Operations, and DoW Information Network Operations.
- Enabling and conducting the actions necessary to provide certification, threat identification, intrusion prevention, intrusion detection, and incident response/recovery for the NIPRNet and the SIPRNet.
- Providing the Command and Control, situational awareness, and defense of the DoW Information Network and Enterprise services across all levels of command: strategic, operational, and tactical boundaries in contested battlespace.
- Supporting the DoW's full spectrum of war fighting, to include support for intelligence and business missions.

DISA executes its Command and Control mission to plan, direct, coordinate, integrate, and synchronize DoW Information Network Operations and Defensive Cyber Operations globally. DISA specifically:

- Manages and executes approximately 200 million managed network assets, over 50,000 Telecommunications Service Orders and circuit actions, 40,000 servers hosting 870 user applications, 17,000 circuits, 55 Satellite Communication gateways, 38 petabytes of storage, 4.5 million DoW identities, 1.6 million to 4.5 million enterprise users, and 1 million to 4.5 million mobility/voice/video/data over IP users.
- Reports blockage and/or tracking of an average of 380 million malicious events monthly.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Increasing cybersecurity threats have expanded the program's Cyberspace Operations mission, necessitating broader defenses (including Enterprise Services) and greater depth in the DoW Information Network Operations / Defensive Cyber Operations mission space. DISA supports USCYBERCOM's mission to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. DISA can meet this expanded need by leveraging its existing enterprise infrastructure.

3. Joint Staff Support Center - (FY 2027: \$30,321 thousand): The Joint Staff Support Center provides 24/7 operational and communications support for Command and Control, Nuclear Command and Control, and National Military Command and Control .It supports the President, Secretary of War, CJCS, Joint Staff, Combatant Commanders, and other National-level leaders through global maintenance of Joint C2 and NC2 systems and cybersecurity oversight. In accordance with CJCS Operating Order (OPOR) 6-19 and CJCS Instruction 3280.01E "National Military Command System," the Joint Staff Support Center Director provides operational direction to create a mission-capable National Military Command Center. These efforts enable the NMCC to perform the National Military Command System's seven mission essential functions and twenty-five mission essential tasks. The Joint Staff Support Center oversees a critical decision support system for the National Military Command Center and the National Joint Operations-Intelligence Center in the Pentagon and at alternative locations. By deterring strategic attacks against the U.S., Allies, and partners through 24/7 support, the Joint Staff Support Center advances and safeguards vital national defense priorities.

The Joint Staff Support Center provides 24/7 monitoring of the National Military Command Center and alternate National Military Command Center locations. It also provides support for nuclear operations for Command and Control, communications, computing, and intelligence systems, enabling worldwide situational monitoring, rapid decision-making, and force direction. These services support strategic threat warning, crisis management, situational awareness, course of action development, and national senior leadership decision-making. Joint Staff Support Center sustains these capabilities through the Global Command and Control System-Joint, the Processing and Display System-Migration, the Nuclear Planning and Execution System, and other systems for the Pentagon and an alternative location to ensure continuity of operations. Joint Staff Support Center prioritizes providing a secure, reliable, and effective nuclear command, control, and communication system by building a resilient, cohesive warfighter support network that overcomes evolving threats.

The Joint Staff Support Center also provides full-service television production and multimedia support to the Secretary of War, CJCS, Joint Staff, and other DoW agencies upon request from Pentagon organizations. This includes remote video and audio recordings, electronic graphics, video teleconferencing guidance, and National Military Command Center secure television system operation. Additionally, the Joint Staff Support Center provides tactical, operational, strategic, and collaborative planning support for various JS IT initiatives, including the National Military Command Center IT Working Group and the Joint Staff IT migration. Personnel also assist the Joint Staff Hampton Roads, Joint Staff Pentagon, and other regional mission partners in transitioning their IT services into DISA-based offerings.

Mission Area: Exploit the DoW Information Network for Improved Decision Making (FY 2027: \$1,343,275 thousand)

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

1. Joint Service Provider - (FY 2027: \$597,943 thousand): The Joint Service Provider (J6 Pentagon) is the exclusive IT service provider for over 30 facilities and a wide variety of DoW personnel throughout the Pentagon Reservation and National Capital Region. Serving over 55,000 customers spanning the Office of the Secretary of War (OSW), Washington Headquarters Services, Army, Joint Staff, and additional onboarded customers, Joint Service Provider employees operate and defend DoW cyber terrain by building, sustaining, supporting, and protecting mission-critical integrated IT systems to "Enable. Every. Mission." Joint Service Provider 's comprehensive services include infrastructure network support, application support, data storage management, defensive cyber operations, cybersecurity compliance, and customer service support to critical DoW facilities.

The Joint Service Provider IT program provides end-user computing capabilities essential for fulfilling component missions. It includes DoW local area networks, computer servers, network storage subsystems, workstations, and desktop applications, processing information at all classification levels across over 110,000 end-user devices. By maintaining IT infrastructure for all key facilities and personnel, the Joint Service Provider enables maximum mission effectiveness for all DoW IT users throughout the National Capital Region. The Joint Service Provider enables cutting-edge IT capabilities, helping warfighters maintain their competitive advantage against emerging threats.

Joint Service Provider also encompasses the Secretary of War Communications Office (SECWARCOMS). The SECWARCOMS serves as the authoritative source for operational and strategic communication requirements supporting the Secretary and Deputy Secretary of War. In accordance with DoW Policy, the Secretary of War must have resilient communication and situational awareness capabilities at the Pentagon, along with access to fully equipped alternative operating facilities and mobile communications during transit. SECWARCOMS provides the SECWAR with these capabilities, enabling the Secretary of War and the Immediate office to coordinate national defense in every scenario.

2. Senior Leadership Enterprise /Logistics Support Activities - (FY 2027: \$340,939 thousand): Details are submitted in appropriately classified exhibits.
3. Combined Advanced Applications - (FY 2027: \$102,549 thousand): The Compartmented Enterprise Services Office provides an accredited Special Access Program IT system, enabling users who operate within a Special Access Program environment to work and communicate. It also facilitates secure cloud communication among executive leaders and mission partners across the DoW and Intelligence Community. Compartmented Enterprise Services Office provides users with email, file storage, wiki, federated search, and print services, while also operating and sustaining the Joint Access Database Environment, an authoritative source for verifying the identity of individuals and programs to networks and systems. Funding sustains Compartmented Enterprise Services Office capabilities and supports incremental improvements based on customer feedback and Special Access Program CIO concurrence.

The Enterprise Financial Accounting System is a Top Secret-Sensitive Access Required Sensitive Compartmented Information financial management system, designed for Sensitive Activities and Special Access Program requirements across the DoW. Funding supports the Enterprise Financial Accounting System's operations and maintenance, licenses, network sustainment, Cybersecurity Service Provider services, and backbone connectivity telecom support. Enterprise Financial Accounting System helps the DoW achieve a clean audit opinion through standardizing processes for recording, reporting and managing financial resources

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

4. Global Command and Control System-Joint - (FY 2027: \$27,287 thousand): The Global Command and Control System-Joint is the Joint Command and Control system of record and an essential component for warfighting situational awareness. It provides an integrated, near real-time picture of the battlespace to support joint and multinational operations across U.S. and coalition networks. Global Command and Control System-Joint displays air, maritime, ground, space, and cyber tracks to aid decision-making. It also provides applications for missile warning, intelligence, targeting, and imagery exploitation. Key strategic, national, theater, and operational decision-makers rely on Global Command and Control System-Joint

The Global Command and Control System-Joint supports Combined Joint All-Domain Command and Control, the modernized military decision-making approach that promotes inter-Service information sharing. Combined Joint All-Domain Command and Control achieve agile and resilient Command and Control across the Services through integrated and synchronized capability development. These Combined Joint All-Domain Command and Control capabilities enable the connection of distributed sensors, intelligence, information, data, and effects from all Services to decision-makers at mission speed. Global Command and Control System-Joint also directly supports building a resilient Joint Force and defense ecosystem, fostering enhanced collaboration and innovative technological integration. It incorporates the core planning and assessment tools for CCMDs, their subordinates, and Joint Task Force Commanders, supporting the readiness of Service requirements and warfighter capabilities. It also provides critical Command and Control capabilities to the Commander-in-Chief, Secretary of War, National Military Command Center, CCMDs, Joint Force Commanders, and Service Component Commanders. Global Command and Control System-Joint users include decision-makers at strategic, national, theater, and operational levels, as well as all CCMDs, worldwide.

The Global Command and Control System-Joint:

- Provides a Common Operational Picture with ground, air, maritime, cyber, and space tracks of U.S., coalition, and enemy forces.
- Provides tactical decision aids and other applications for common operational picture management and situational awareness.
- Functions as the system of record for Theater Missile Warning, which provides alerts and displays for real-time missile events.
- Displays launch points, missile locations, threat fans, and projected impact points.
- Provides intelligence support to Command and Control operators with national and tactical intelligence data from Defense Intelligence Agency's 's Modernized Integrated Database, still and motion imagery, and other intelligence sources.

The Joint Staff Support Center provides 24/7 support to DoW components around the globe. Support efforts include:

- Global Tier II technical support to over 660 sites.
- Operational monitoring and reporting of 51 critical sites.
- Global Common Operational Picture technical support and management of National Capital Region Global Common Operational Picture servers.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

5. Joint Planning and Execution Services - (FY 2027: \$33,743 thousand): DISA, via the Joint Planning and Execution Services Program Management Office provides information technology capabilities supporting DoW's Joint Planning Process. These capabilities support force planning, deployment planning, allocation of forces, execution, and Global Force Management processes for military operations, integral to the Joint Command & Control mission.

The Joint Planning and Execution Services program maintains and sustains two operational systems:

Joint Capabilities Requirements Manager: The Joint Capabilities Requirements Manager is a web-based application and database that facilitates the Global Force Management Allocation Plan. It enables CCMDs to draft, staff, store, and submit force requirements for ongoing and emerging military operations, contingency plans, and military exercises worldwide. Joint Capabilities Requirements Manager is vital for managing complex global force requirements and tracking the distribution of U.S. military forces among the CCMDs, thereby fulfilling its mission.

Joint Planning and Execution Services: The Joint Planning and Execution Services is the critical Joint Command & Control system, providing automated force planning and execution capabilities necessary for simultaneous and resource-informed planning activities. Joint Planning and Execution Services is a collection of capabilities supporting joint policies, processes, procedures, and reporting structures, backed by communications and information technology used by the Joint Planning and Execution Community. Joint Planning and Execution Community leverages these capabilities to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities for joint operations and exercises.

6. Mission Partner Environment - (FY 2027: \$216,692 thousand): The Mission Partner Environment portfolio supplies the foundational technology for the DoW to collaborate effectively with a wide range of Mission Partners during all phases of operations. These partners can include other federal agencies, state and local governments, private entities, allies, and organizations supporting multi-national treaties. As the primary operating framework for Command and Control, the Mission Partner Environment enables seamless information sharing for planning and execution across the full spectrum of military operations. Mission Partner Environment capabilities are specific technologies that support the overall framework. Successful recent applications of the Mission Partner Environment include coordinating communications for allied forces in support of Ukraine and establishing a common information-sharing environment for the United States, Canada, and Mexico during the World Cup.

Sustained Mission Partner Environment operations are vital to ensuring combined Command and Control of coalition forces, secure information sharing, and the effective use of military power in an increasingly complex global security environment. Some of the specific Mission Partner Environment capabilities DISA supports include:

- **Pegasus:** Provides a means for disseminating classified information between Five Eye nations. It includes operationalized Five Eye services, including web browsing, email with attachments, chat, SharePoint, and voice.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

- **Combined Federated Battle Laboratories Network:** A testing network environment used to facilitate the resolution of interoperability issues between the U.S. and coalition partner systems.
- **Five Eye C41 Service Operations Group:** Manages and tracks the end-to-end lifecycle of incidents including but not limited to, reviewing incident records to ensure they include all the necessary information. Five Eye C41 Service Operations Group: also assigns tasks to the nations' National Networks Operation Centers for incident investigation, diagnosis, and resolution.
- **Coalition Information Environment:** Coalition Information Environment is the full build out of the Joint Operational Edge – Coalition Environment concept for both Command and Control and collaboration capabilities. Joint Operational Edge – Coalition Environment was a prototype for secure, cloud-based Command and Control coalition capabilities, focused on USINDOPACOM. Joint Operational Edge – Coalition Environment leveraged security from Thunderdome and Enterprise Identity, Credential, and Access Management to grant appropriate access to infrastructure and the Maven Smart Systems artificial intelligence platform.

During FY 2027, DISA is undergoing a major effort to operationalize and sustain Coalition Information Environment. Coalition Information Environment will provide a secure, unified hybrid cloud environment for both Command and Control and collaboration at the Secret and below levels. Coalition Information Environment will include core compute and transport infrastructure, provider functionality, and end user applications. Coalition Information Environment is replacing the Air Force's Secret and Below Releasable Environment for collaboration capabilities and building out the Joint Operational Edge – Coalition Environment Command and Control capabilities. DISA is currently determining the prioritization for global scaling across USEUCOM, USCENTCOM, and USSOUTHCOM.

The Coalition Information Environment is built on a resilient, three-tiered architecture to ensure data availability from the enterprise to the tactical edge:

1. Enterprise Core (Strategic): The global backbone providing centralized services and data synchronization for the entire coalition.
2. Theater: Powerful, in-theater data centers that support a specific Combatant Command (e.g., INDOPACOM) and are designed to operate independently for resilient Command and Control.
3. Regional (Edge): Lightweight, mobile hardware that extends the network to forward-deployed warfighters, enabling real-time data processing in potentially disconnected environments.

DISA is executing the Coalition Information Environment in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. Coalition Information Environment contributes to Mission Network as a Service by providing a cloud-based central hub for conducting Command and Control and collaboration activities with Mission Partners.

- **Global Network Operations and Security Center:** The Global Network Operations and Security Center is the single authority for the Coalition Information Environment program's operations, security, and maintenance, providing a unified service desk for all coalition partners. Global Network Operations and Security Center operations stretch across incident and problem management, change and

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

configuration management, cybersecurity defenses, and general service management, ensuring maximal availability, resilience, and security.

As a critical enabler of mission success, the DoW Mission Partner Environment program is constantly evolving. DISA continues to refine and expand these capabilities to meet the demands of a complex operational landscape and to advance the Secretary of War's priority of reestablishing deterrence through allied coordination. Ultimately, the Mission Partner Environment strengthens the DoW's alliances, enhances its competitive edge, and improves its ability to achieve mission objectives in joint and combined operations.

7. Other Programs - (FY 2027: \$24,122 thousand): These funds cover the infrastructure and support costs for DISA's interoperability facility in the National Capital Region, including facility operations, utilities, business management, and IT support. This investment enables the DISA interoperability facility to operate more efficiently and effectively in pursuit of national defense priorities.

Mission Area: Deliver Capabilities Effectively/Efficiently (FY 2027: \$195,525 thousand)

1. Shared Services Units/Program Executive Offices - (FY 2027: \$124,295 thousand): This activity provides essential operational support to DISA worldwide, enabling the agency to deliver critical capabilities to its programs and business areas. It funds foundational elements such as financial management, information technology, strategic planning, personnel security, facilities, logistics, and acquisition support. DISA is modernizing its internal operations by deploying advanced technical solutions for software licensing (DoW365), contract provisioning, human resources, and financial management. These improvements strengthen readiness by ensuring continuous, reliable operational capabilities and enabling DISA to effectively support the Warfighter. Key efforts include:
 - **Commodity IT Support:** Funding DISA's internal network operations, maintenance, and sustainment; connectivity to NIPRNet and SIPRNet via DoDNet; global service desk support; Microsoft 365 licensing; and other services necessary to maintain a securely connected and productive workforce.
 - **Data Management and Governance:** Managing DISA's evolving data architecture, data governance, metadata collection, data platform design, systems design, and interface design. This includes enforcing data management disciplines and enhancing data quality to enable digital transformation and outmaneuver adversaries in the digital battlespace.
 - **Compliance and Oversight:** Managing records declassification, IT commodity tracking, policy oversight, and compliance reviews.
 - **Human Resources Support:** Operating and maintaining human resources systems that track employee attendance, ensure continuity of operations, and facilitate compliance with personnel security requirements and the Executive Order on Return to In-Person Work.
 - **Financial Management:** Operating and maintaining financial systems crucial for prudent resource management, auditability, preventing improper payments, and providing leadership with data for efficient agency management. This includes performing critical oversight functions to mitigate fraud, waste, and abuse, reduce costs, and strengthen internal controls. DISA is aggressively working

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

toward a clean financial statement audit to ensure resource accountability, aligning with the Secretary of War's priority of rebuilding the military.

- **Training and Certification:** Managing Information Technology/Cyber, financial management, acquisition, and congressionally mandated trainings and certifications.
- **Facilities and Logistics:** Efficiently administering real property services, assets, and logistical processes to provide a safe, sustainable, and optimized environment, including maintaining secure office space at DISA Headquarters and Joint Service Provider leased facilities to support the Executive Order on Return to In-Person Work.

The FY 2027 request for Shared Services includes \$124,295 thousand of discretionary

2. Management Headquarters - (FY 2027: \$38,859 thousand): This funding supports key oversight organizations that provide guidance and direction for DISA's acquisition, financial, and personnel activities. Command and executive staff sustain DISA's continuous operation and secure the reliability of its global enterprise, directly supporting the joint warfighter, national-level leaders, and mission and coalition partners across the full spectrum of operations.

Management Headquarters provides critical support to military, civilian, and contractor personnel across twenty-five states, the District of Columbia, and eight countries worldwide. Headquarters personnel develop and administer financial and human resources policy, conduct audits and reviews to safeguard agency resources and processes, and provide legal counsel to ensure DISA operates in accordance with its statutory authorities. They are actively identifying savings and organizing the agency to comply with Presidential Executive Orders promoting efficient operations and preparing the agency for a clean audit opinion.

3. Pentagon Reservation Maintenance Revolving Fund - (FY 2027: \$32,371 thousand): Section 2674 of title 10, U.S. Code, established the Pentagon Reservation Maintenance Revolving Fund. This fund authorizes the Secretary of War to set rates, collect charges, and make payments for facilities-related services (space, protection, maintenance, construction, repairs, and alterations) provided at the Pentagon Reservation. This activity funds DISA's utilization of Pentagon Reservation Maintenance Revolving Fund services.

Mission Area: Special Mission Area (FY 2027: \$620,659 thousand)

1. White House Communications Agency - (FY 2027: \$589,474 thousand): The White House Communications Agency is a joint service military agency under White House Military Office operational control, operating per the 2006 NDAA, Public Law 109-163. It provides 24/7 worldwide classified and unclassified information services to the POTUS, VPOTUS, White House Military Office, and others as directed by the President through the White House Director of Technology. Operating primarily in the National Capital Region, White House Communications Agency also supports Presidential Information Technology Community networks at Camp David, second residences, worldwide travel sites, Executive Office of the President and White House Military Office offices, vehicles, aircraft, alternate Continuity of Operations and Continuity of Government, the Signal Support Element, and other Head of State services. Through four core mission areas—Information Systems Services,

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Customer Service, Deployable Communications, and Visual Information Services— White House Communications Agency ensures unified communications at all classification levels, enabling the President to communicate with anyone, anywhere, under any condition. This secure communication capability is crucial for ensuring warfighters can respond to emerging threats in real time under the Commander-in-Chief's leadership.

In FY 2027, 1. White House Communications Agency will be addressing limitations in White House Communications Agency and DoW communications systems. Details are classified and available on request.

2. White House Situation Support Staff - (FY 2027: \$29,638 thousand): White House Situation Support Staff is responsible for providing financial and personnel resources to support and manage critical information technology, audiovisual, and communications functions within the National Security Council, including those performed by the White House Situation Room.

The White House Situation Room provides 24/7 global situational awareness, crisis management facilitation, secure conference facilities, emergency actions support, and executive communications directly for the President as Commander-in-Chief, Head of State, and Chief Executive, while also supporting the Vice President, National Security Advisor, National Security Council staff, and select senior White House staff. The funding sustains operations including applications and tools for White House Situation Room watch floor operations and National Security Council decision making, telecommunications systems operations and maintenance at White House Situation Room locations (including Continuity of Operations and Continuity of Government , support), global forward deployment for special mission travel, facility sustainment, and the budgeting, acquisition, logistics, and administrative activities required to execute these critical responsibilities

3. Communications Management Control Activity - (FY 2027: \$1,547 thousand): The Communications Management Control Activity provides communications support to the United States Secret Service for Presidential campaigns, dignitary protective duties, and National Special Security Events, as well as supporting the Joint Staff/J3, Joint Chiefs of Staff Special Events, and Joint Directorate of Military Support for special events. Under Public Law 106-544, the United States Secret Service coordinates, plans, exercises, and implements security for National Special Security Events, while DoW Directive 3025.13 mandates DISA support to the Communications Management Control Activity.

The FY 2026 spend plan amount for O&M includes \$2,955,565 thousand of discretionary and \$53,000 thousand of mandatory (reconciliation) for a total of \$3,008,565 thousand.

The FY 2027 request for O&M Non-Cyber includes \$3,873,222 thousand of discretionary \$12,385,145 thousand of mandatory for a total of \$16,258,367. The mandatory funds the DISA are funding to address the critical infrastructure capability gaps required to support Sovereign Artificial Intelligence across the DoW and critical deferred maintenance projects including, but not limited to, mechanical, plumbing, structural, architectural, fire alarm/suppression and Sensitive Compartmented Information Facility upgrades. The FY 2027 funds are different from the FY 2026 mandatory funds that support Enterprise Financial Accounting System and White House Communication Agency Classified support.

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

II. Force Structure Summary:
N/A

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

III. Financial Summary (\$ in Thousands)

	FY 2025 <u>Actuals</u>	Budget <u>Request</u>	FY 2026 <u>Congressional Action</u>		Current <u>Enacted</u>	FY 2027 <u>Request</u>
			<u>Amount</u>	<u>Percent</u>		
<u>A. BA Subactivities</u>						
1. Transition to Data-Centric Environment	\$336,759	\$483,201	\$-52,416	-10.85%	\$430,785	\$526,607
2. Eliminate Bandwidth Constraints	\$422,952	\$721,834	\$-32,928	-4.56%	\$688,906	\$967,085
3. DoWIN Network Operations & Defense	\$197,558	\$214,767	\$1,350	0.63%	\$216,117	\$220,071
4. Exploit the DoWIN for Improved Decision Making	\$1,056,235	\$1,064,272	\$-6,935	-0.65%	\$1,057,337	\$1,343,275
5. Deliver Capabilities Effectively/Efficiently	\$278,963	\$210,637	\$3,800	1.80%	\$214,437	\$195,525
6. Special Missions	\$343,169	\$347,848	\$135	0.04%	\$347,983	\$620,659
Total	\$2,635,636	\$3,042,559	\$-86,994	-2.86%	\$2,955,565	\$3,873,222

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

<u>B. Reconciliation Summary</u>	Change	Change
	<u>FY 2026/FY 2026</u>	<u>FY 2026/FY 2027</u>
BASELINE FUNDING	\$3,042,559	\$2,955,565
Congressional Adjustments (Distributed)	30,000	
Congressional Adjustments (Undistributed)	-97,255	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	-19,739	
Fact-of-Life Changes (2026 to 2026 Only)	0	
SUBTOTAL BASELINE FUNDING	2,955,565	
Supplemental	0	
Reprogrammings	0	
Price Changes		51,638
Functional Transfers		134,509
Program Changes		731,510
CURRENT ESTIMATE	2,955,565	3,873,222
Less: Supplemental	0	
NORMALIZED CURRENT ESTIMATE	\$2,955,565	\$3,873,222

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

FY 2026 President's Budget Request (Amended, if applicable)	\$3,042,559
1. Congressional Adjustments	\$-86,994
a) Distributed Adjustments	\$30,000
1) Program increase - 4ENO transition costs	\$23,000
2) Program increase - JSC consolidation	\$7,000
b) Undistributed Adjustments	\$-97,255
1) Historical Unobligated Balances.....	\$-97,255
c) Adjustments to Meet Congressional Intent.....	\$0
d) General Provisions.....	\$-19,739
1) Sec. 8136 Savings from Efficiencies	\$-19,739
FY 2026 Appropriated Amount	\$2,955,565
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) 2027 Budget Estimates**

c) Emergent Requirements.....	\$0
FY 2026 Baseline Funding.....	\$2,955,565
4. Reprogrammings (Requiring 1415 Actions)	\$0
a) Increases.....	\$0
b) Decreases	\$0
Revised FY 2026 Estimate	\$2,955,565
5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings.....	\$0
a) Less: Supplemental Funding.....	\$0
FY 2026 Normalized Current Estimate	\$2,955,565
6. Price Change.....	\$51,638
7. Functional Transfers.....	\$134,509
a) Transfers In	\$134,509
1) Chief Digital and Artificial Intelligence Office (CDAO) to DISA Mission Partner Environment Transfer	\$6,000
Increase due to non-pay funding being transferred from the Chief Digital and Artificial Intelligence Office to DISA to support the Mission Partner Environment. Following a consensus recommendation to the Deputy Secretary, the DoW Chief Information Officer has directed the transfer of responsibilities for Mission Partner Environment operations, sustainment, and development from the CDAO to the DoW Chief Information Officer (CIO) and DISA. (FY 2026 Baseline: \$0 thousand)	
2) Department of the Air Force to DISA Mission Partner Environment Transfer	\$128,509

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

\$126,715 thousand increase due to non-pay funding being transferred from the Department of the Air Force to DISA to support the Mission Partner Environment. Following a consensus recommendation to the Deputy Secretary, the DoW CIO has directed the transfer of responsibilities for Mission Partner Environment operations, sustainment, and development from the Department of the Air Force to the DoW CIO and DISA. This increase will enable DISA to sustain existing capabilities, including Pegasus, the Combined Federated Battle Laboratories Network, and the Five Eye C41 Service Operations Group, and develop new capabilities as needed. Capability development in FY 2027 centers on the Coalition Information Environment, which will provide both the Command and Control capabilities developed during the Joint Operational Edge-Coalition Environment pilot and collaboration partners to coalition forces. The requested funding for FY 2027 will ensure the Mission Partner Environment remains a secure, interoperable, and effective platform for mission partner collaboration.

\$1,794 thousand, nine Full-Time Equivalent (FTEs) increase to support Mission Partner Environment. This increase is the result of funding being transferred from the Department of the Air Force to DISA to support the Mission Partner Environment. Following a consensus recommendation to the Deputy Secretary, the DoW CIO has directed the transfer of responsibilities for Mission Partner Environment operations, sustainment, and development from the Department of the Air Force to the DoW CIO and DISA.
(FY 2026 Baseline: \$0 thousand; +9 FTEs)

b) Transfers Out	\$0
8. Program Increases	\$900,167
a) Annualization of New FY 2026 Program	\$0
b) One-Time FY 2027 Increases	\$0
c) Program Growth in FY 2027	\$900,167
1) Fourth Estate Network Operations Non-Pay	\$72,000
<p>\$72,000 thousand increase to support the critical planning and design work required to migrate the 11 CCMDs from their legacy networks onto a single network for their core IT that leverages DoDNet's infrastructure: Combatant Command Network Optimization (CCMDNet). The migration of CCMDs to CCMDNet will follow the same pattern as the migration of DAFAs to DoDNet. DISA will first conduct site surveys to assess the status of the IT equipment at each Combatant Command. Then DISA will identify the specific IT equipment required for successful connection of each Combatant Command to CCMDNet.</p>	

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Centralized funding for planning and design will expedite work and help DISA achieve FY 2028 CCMDNet migration targets.

DISA is developing CCMDNet in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. CCMDNet contributes to Mission Network as a Service by providing the network infrastructure the Combined Joint Force will use to access DISN and Command and Control services.
(FY 2026 Baseline: \$145,667 thousand)

2) DoW Teleport Program Non-Pay\$27,958

\$17,958 thousand increase for sustainment of the Resilient Ground Infrastructure initiative; primarily, the installation, warranty, and maintenance activities of Medium Earth Orbit Integration, the installation and warranty of hundreds of Enterprise Satellite Communications Modems, and additional Joint Satellite Communications Teleport - Satellite Communications Enterprise expansion nodes. Operational support is necessary to sustain Teleport's expanded satellite communications infrastructure, which now includes more sites and enhanced capabilities. Expanding the redundancy of the Teleport directly supports key Secretary of War priorities by modernizing infrastructure, ensuring reliable global connectivity for operational forces, and strengthening deterrence with resilient, secure communications.

\$10,000 thousand increase for critical enhancements for the Joint Management Tool, upgrading it to incorporate advanced commercial Satellite Communications providers, including proliferated Low Earth Orbit constellations, and the U.S. Space Force's new Protected Tactical Waveform capability. These upgrades will provide worldwide anti-jam communications for tactical warfighters and enable the efficient provisioning of new Satellite Communications options, significantly improving readiness and rapid deployment. The project also includes integrating the Joint Management Tool with regional communication hubs, such as the Naval Computer and Telecommunications Area Master Station, to further diversify Satellite Communications resources. Finally, DISA will develop a new Impact Level 5 instance for the Automated Resource Assignment and Automated Resource Requests capabilities to securely provision Satellite Communications resources to mission partners and allies, directly supporting the SECWAR's priority of reestablishing deterrence by working closely with international allies and partners to mitigate adversarial aggression.
(FY 2026 Baseline: \$55,103 thousand)

3) Global Command and Control System - Joint Non-Pay\$108

Increase due to higher operational and sustainment costs as the Common Operational Picture capability is sustained within the Global Command and Control System - Joint web platform. The Common Operational Picture provides a comprehensive, unified view of the operational environment by fusing and displaying the geographic locations of friendly, hostile, and neutral forces with real-time intelligence and environmental

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

data.

(FY 2026 Baseline: \$10,378 thousand)

4) Management Headquarters Non-Pay.....\$397

Increase for oversight efforts implemented by the Director's Office to identify and eliminate wasteful or redundant practices within its personnel operations. This initiative will enable the Department to allocate resources more efficiently and better support the warfighter.

(FY 2026 Baseline: \$10,607 thousand)

5) Other Programs Non-Pay.....\$668

Increase for increasing information technology, acquisition, and logistics support costs. These are required to maintain a cutting-edge lab environment which fosters rapid innovation, experimentation, and development of advanced technologies.

(FY 2026 Baseline: \$15,907 thousand)

6) Joint Service Provider Non-Pay.....\$10,100

\$4,300 thousand increase supports services for additional users and rapid capability delivery to special interest panels, initiatives and sites outside the National Capital Region that operate on behalf of the Secretary of War and Deputy Secretary of War that require remote site support to extend both DISA and non-DISA network connectivity extensions up to the Top-Secret classification level.

\$4,100 thousand increase provides additional Technical Surveillance Countermeasures Support for hold rooms and travel. By presidential directive, SECWARCOMs must deliver uninterrupted communications capabilities to all Secretary of War and Deputy Secretary of War locations 24/7 regardless of location or classification. New mandates call for SECWARCOMs to deploy sensitive countermeasures equipment not just to hotels communications rooms but also to temporary Hold Rooms in forward deployed locations. Technical Surveillance Countermeasures Support personnel must deploy with the advanced team and cleared Hold Rooms must remain under 24/7 watch until released back to host. Additionally, increased requirement of establishing Top Secret/Sensitive Compartmented Information voice, video, and data in secondary locations while on travel has driven an increase for desktop telecommunication services previously limited to centralized comms rooms.

\$1,700 thousand increase sustains an increase of licenses across the SWC catalog for new users, all-hazards readiness efforts that include uninterrupted mobile communications capabilities and continuity site requirements to ensure SECWAR operational readiness to continue Primary Mission Essential Functions regardless of threat or location.

(FY 2026 Baseline: \$518,571 thousand)

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

- 7) Defense Information Systems Network Infrastructure Services Non-Pay\$3,303
 Increase due to coverage of the DISA CIO portion of DISN IS, which enables continued use of Defense Information Systems Network circuits. Defense Information Systems Network Infrastructure Services is the bill Defense Information Systems Agency pays for these circuits. The funding covers services such as Global Content Delivery Services, Global Video Services, Low Speed Time Division Multiplex, and Enhanced Mobile Satellite Services.
 (FY 2026 Baseline: \$24,624 thousand)
- 8) Joint Planning and Execution Services Non-Pay\$3,741
 Increase in support of Joint Planning and Execution Services artificial intelligence enablement, which will integrate artificial intelligence to create a robust, data-driven solution for Global Force Management. An artificial intelligence capability will analyze vast datasets to optimize logistics, enhance data-driven force planning, improve threat detection, and reduce operational costs. By driving automation and efficiency, this initiative will significantly strengthen the DoW's ability to rapidly plan, deploy, and sustain forces, ultimately bolstering national security and improving system flexibility and cybersecurity.
 (FY 2026 Baseline: \$24,379 thousand)
- 9) Data-Centric Enterprise Services Non-Pay\$5,702
 Increase for the Defense Emergency Services IP Network, which is introducing a modern, highly reliable, and secure data network for all its emergency communications, much like a private, military-grade version of the system states use for 911 calls. DISA is piloting Defense Emergency Services IP Network in FY 2027. Funding will support the core network infrastructure and support needed for one pilot enclave, which includes contract labor support, security services, and the operational cost of the pilot program. By adopting an Emergency Services IP Network, the DoW can significantly enhance its communication infrastructure by moving from legacy systems to a more resilient, reliable, and scalable IP-based network. The Defense Emergency Services IP Network will enable seamless, real-time data sharing and interoperability across all agencies and jurisdictions, from field operations to command centers, improving coordination and response times during crises or disasters across different bases and branches.
 (FY 2026 Baseline: \$134,168 thousand)
- 10) White House Situation Support Staff Non-Pay\$7,164
 Increase due to sustainment requirements for White House Situation Room IT infrastructure following significant renovation. Dedicated funding supports modernized operations providing Senior Leadership with uninterrupted, secure, and high-speed communication. Additionally, this infrastructure enables informed and timely decision-making in response to evolving foreign policy and military challenges.
 (FY 2026 Baseline: \$19,229 thousand)
- 11) Combined Advanced Applications Non-Pay.....\$30,493

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

\$3,575 thousand increase to support the Compartmented Enterprise Services Office in providing an accredited Special Access Program IT system. This system enables users to work and communicate securely within a Special Access Program environment. The funding sustains CESO capabilities and supports incremental improvements based on customer feedback and Special Access Program CIO concurrence.

\$26,918 thousand increase for the Enterprise Financial Accounting System, which will be operational in FY 2027 for DISA and the Missile Defense Agency. The Enterprise Financial Accounting System marks a significant advancement in modernizing the DoW's financial operations, enhancing security of classified information, and supporting the DoW's FY 2028 clean audit objectives. As a Top Secret-Sensitive Access Required Sensitive Compartmented Information financial management system, the Enterprise Financial Accounting System is designed for Sensitive Activities and Special Access Program requirements across the DoW. This increase provides DISA with a stable funding profile to manage the Enterprise Financial Accounting System program as additional DoW Agencies migrate to the Enterprise Financial Accounting System. The funding supports the system's operations and maintenance, licenses, network sustainment, Cybersecurity Service Provider services, and backbone connectivity telecom support. Migration to the Enterprise Financial Accounting System facilitates the retirement of legacy systems and helps the DoW achieve a clean audit opinion through standardizing processes for recording, reporting and managing financial resources.

(FY 2026 Baseline: \$66,553 thousand)

12) Defense Spectrum Organization Non-Pay\$10,094

Increase to operationalize and sustain modernized Electromagnetic Spectrum capabilities as they are deployed. Electromagnetic Spectrum Modernization involves transitioning legacy Electromagnetic Spectrum applications across the DoW to one foundational platform architecture to enable real-time processing, automation, Artificial Intelligence/Machine Learning , and dynamic spectrum sharing. Electromagnetic Spectrum Modernization will improve management, frequency assignments, situational awareness, decision support, and Command and Control of the Electromagnetic Spectrum assets to accelerate superiority on the battlefield. Electromagnetic Spectrum Modernization will also enable CCMDs and other DoW components to conduct joint planning, coordination, and control of the Electromagnetic Spectrum. The Joint Operational Edge (JOE) capability will ensure resilient Electromagnetic Spectrum operations in Denied, Degraded, Intermittent, and Limited (DDIL) environments, which have low bandwidth, high latency, and limited connectivity.

(FY 2026 Baseline: \$31,034 thousand)

13) DOW Information Network Operations Non-Pay\$10,109

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Increase for realignment of resources from other DISA portfolios to consolidate the financial management of the Global Solutions Management Operations contract and other network operations support. The Global Solutions Management Operations contract provides operations, planning and execution services, and cybersecurity services, ensuring the DoW has the right people and processes in place to manage its global network effectively. Funding is realigned from Field Commands and Field Offices (\$8,331 thousand) and Shared Services (\$1,778 thousand).
(FY 2026 Baseline: \$33,912 thousand)

14) Senior Leadership Enterprise Non-Pay\$12,556

This program/mission is classified. Details provided for this program are submitted in appropriately classified DoW exhibits.

(FY 2026 Baseline: \$313,457 thousand)

15) Civilian Compensation\$17,825

\$7,192 thousand, 30 FTEs increase for the White House Communications Agency to address critical manning and resourcing shortfalls due to sustained increase in operational tempo including higher volume of travel, expanded user base and evolving capabilities in support of White House travel.

\$6,075 thousand increase strengthens the Department’s ability to recognize and reward the civilian workforce whose expertise and continuity underpin mission success. Expanded award capacity helps retain the talent that sustains warfighter readiness, drives innovation, and ensures uninterrupted support across the enterprise. Investing in civilian recognition directly reinforces the workforce that delivers stability, operational excellence, and long term capability for the Department.

\$2,764 thousand, ten FTEs increase to support the creation of the White House Military Office of Technology. Five of these FTEs are specialized Headquarters Equivalents (HQEs) to meet highly sensitive White House needs and thus more expensive than the FY 2027 DISA AAR. This program/mission is classified. Details are available on request.

\$1,794 thousand, nine FTEs increase for Critical Time Dissemination to support the DoW Information Network’s precision timing network. These personnel deploy globally to inspect, operate, and upgrade the 46 Defense Regional Clocks and 30 Timing and Synchronization System Capability suites, staff a perpetual test lab to ensure system optimization and integrate advanced technologies. A dedicated team also maintains a watch-floor presence, monitoring and coordinating timing for mission-critical assets to guarantee a secure and resilient network.

(FY 2026 Baseline: \$447,735 thousand; 2,239 FTEs; +49 FTEs)

16) DoW Enterprise Cloud Computing Ecosystem Non-Pay\$101,114

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

\$5,000 thousand increase supports the installation of dedicated, high-bandwidth circuits to connect to the Joint Warfighting Cloud Capability and for the build-out of secure floor space to host Cloud Service Provider Points of Presence. This investment is critical to enabling the DoW to fully leverage the capabilities of the Joint Warfighting Cloud Capability, a multi-vendor, multi-cloud enterprise solution designed to provide warfighters with secure and resilient cloud services from the headquarters to the tactical edge.

\$13,600 increase supports DISA installing Joint Unmanaged Landing Zones for all four Joint Warfighter Cloud Contract hyperscale Cloud Service Providers at the Impact Level Six level. These landing zones will function as accredited, pre-approved security boundaries with corresponding network gateways on SIPRNet. This will standardize how cloud applications are secured, eliminating the need for slow and costly individualized security deployments for each new application. This environment will provide the cloud providers with an accelerated connection to the warfighter network and enable communications between them, creating a true hybrid solution.

\$82,514 thousand increase supports DISA adding artificial intelligence acceleration hardware to existing Joint Operational Edge sites overseas, putting powerful artificial intelligence tools directly in the hands of tactical mission partners. This hardware will include Graphics Processing Units , a specialized electronic circuit designed for rapidly handling complex processes for artificial intelligence workloads. Unlike Central Processing Units , Graphics Processing Units use thousands of smaller cores to process multiple tasks simultaneously, making them essential for AI, machine learning, and high-performance computing. These combined enhancements will directly strengthen the warfighter by dramatically expanding their ability to process information and make key decisions within their area of responsibility. This initiative will directly support the Secretary of War's priorities by rebuilding the overseas digital infrastructure, restoring readiness by giving forward troops faster access to data and artificial intelligence, and reestablishing deterrence by deploying cutting-edge technology to the tactical edge.
(FY 2026 Baseline: \$83,422 thousand)

17) Mission Partner Environment Non-Pay\$82,183
Increase to operationalize and sustain the Coalition Information Environment. Coalition Information Environment provides a secure, unified hybrid cloud environment for sharing information at the Secret and below levels with mission partners. It is replacing the Air Force's legacy Secret and Below Releasable Environment for collaboration capabilities and fully building out the Command and Control capabilities developed by the Joint Operational Edge -Coalition Environment pilot. Coalition Information Environment is starting at the SECRET level with plans to expand to unclassified communication levels. Funding supports the following activities: creating the operational/technical baseline to include automation and infrastructure as code, integrating multiple existing commercial-off-the-shelf capabilities; deploying and sustaining five nodes that deliver capability across theater and enterprise; establishing and operating the Global Network

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Operations and Security Center to provide centralized monitoring, cybersecurity, and management for the entire environment; and establishing and operating fully functioning tiered support. DISA is executing Coalition Information Environment in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. Coalition Information Environment contributes to Mission Network as a Service by providing a cloud-based central hub for conducting Command and Control and Collaboration activities with Mission Partners.
(FY 2026 Baseline: \$0 thousand)

18) White House Communications Agency Non-Pay\$247,222
Increase to support a White House initiative to address limitations in White House Communications Agency and DoW communications systems. This program/mission is classified. Additional details are available on request.
(FY 2026 Baseline: \$278,901 thousand)

19) Defense Information Systems Network Enterprise Activities Non-Pay.....\$257,429
\$96,272 thousand increase to eliminate critical technical debt across the DoW Information Network. Over time, DISA has accumulated tech debt related to critical Defense Information Systems Network components and the network still include legacy Time-Division Multiplexing systems. Time-Division Multiplexing networks face obsolescence as vendors are ending support. This funding will accelerate transition to a modern, all Internet Protocol and optical core, mitigating security risks and performance limitations. This includes delivery of new service delivery nodes that will extend the Defense Information Systems Network directly to the warfighter and DISA mission partners at strategic locations. Components being upgraded include nodes, routers, switches, controllers, security devices, and terminals. O&M funding will cover maintenance, repair, warranties, components below the procurement threshold, and the execution of necessary site, power, and infrastructure upgrades. This modernization strengthens the Defense Information Systems Network by guaranteeing the communications backbone is always available for the warfighter, preventing mission failure due to network outages.

\$57,512 thousand increase to purchased communications (non-fund) for Defense Information Systems Network Resiliency. This program/mission is classified. Additional details are available on request.

\$46,920 thousand increase for enhancement and sustainment of INDOPACOM IP Networks. DISA will be conducting optical and Internet Protocol tech refresh and modernization, which includes extending the modern, high-speed network directly to warfighters by deploying new Service Delivery Nodes, which are the core IP and optical infrastructure of Defense Information Systems Network. DISA is building out the network's footprint and placing this advanced hardware in strategic locations, with a primary emphasis on the Pacific theater. This ensures that the advanced capabilities of the modernized Defense Information Systems

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Network are not just confined to the core network but are accessible at the tactical edge where missions are executed. This effort strengthens the DoW by providing forward-deployed forces and mission partners with the robust, high-bandwidth connectivity required for data-intensive, multi-domain operations. It directly supports the Secretary of War's priority to Rebuild the Military by fielding tangible, cutting-edge infrastructure to critical regions and helps Reestablish Deterrence by creating a physically resilient and technologically superior network presence in the Pacific, signaling a credible and enduring commitment to the region. Funding will purchase warranties, system components below the procurement threshold, planning and design and ongoing maintenance and repair.

\$20,379 thousand increase for continued sustainment of the initial operating capability of Classified Voice and Video. Classified Voice and Video provides communication across multiple classification levels on a single platform, supporting the nation's Nuclear Command, Control, and Communications system. The nation's Nuclear Command, Control, and Communications system is critical for maintaining the readiness of U.S. nuclear forces under all circumstances, including during and after nuclear or non-nuclear attacks. The increase will sustain the initial capability, which includes a pre-production environment, three geographically dispersed sites, a network operations center, and a security operations center, and will also fund the deployment of Classified Voice and Video to three additional sites to expand the capability.

\$15,852 thousand increase for the Critical Time Dissemination program will provide dedicated funding to sustain and enhance the DoW's timing infrastructure, directly supporting national defense priorities. This funding will sustain 46 Defense Regional Clocks and 30 Timing and Synchronization System Capability suites and establish and operate a permanent test lab for system optimization and security compliance. The investment also enables upgrades with anti-spoofing technologies, central monitoring, GPS-independent time-holding capabilities, and expands the infrastructure to meet growing demand for precision time. Ultimately, this ensures a resilient time distribution capability across the DoW Information Network enterprise. DISA is developing Critical Time Dissemination capabilities in accordance with the Mission Network as a Service framework, which aims to deliver a unified, secure, and agile Secret environment for the Combined Joint Force. Critical Time Dissemination contributes to Mission Network as a Service by proving the Combined Joint Force with precision timing when using Defense Information Systems Network and Command and Control services to conduct sensitive targeting operations.

\$12,007 thousand increase for Resilient Ground Infrastructure sustainment. As DISA expands the Airborne Intelligence Surveillance and Reconnaissance footprint, it requires increased sustainment funds to keep the equipment operational to facilitate the Airborne Intelligence Surveillance and Reconnaissance data transport to the warfighter. The Resilient Ground Infrastructure initiative aims to expand the reach, resiliency, and redundancy of Airborne Intelligence Surveillance and Reconnaissance by constructing additional Ground stations that support the transmittal of Airborne Intelligence Surveillance and Reconnaissance -compatible

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

frequencies. Airborne Intelligence Surveillance and Reconnaissance allows for cross-functional communication in direct support of CCMDs and boots on the ground efforts.

\$8,487 thousand increase for the deployment of Outside the Continental United States (OCONUS) Classified Mobility Gateways. The deployment of these gateways will enhance network accessibility and improve the user experience, as well as enable DISA's infrastructure to meet new Commercial Solutions for Classified Continuous Monitoring Annex requirements. To sustain a secure environment, these Gateways incorporate Mobile Access Capability Package controls into the network architecture.
(FY 2026 Baseline: \$388,037 thousand)

9. Program Decreases	\$-168,657
a) Annualization of FY 2026 Program Decreases	\$0
b) One-Time FY 2026 Increases	\$0
c) Program Decreases in FY 2027	\$-168,657
1) Joint Service Provider (JSP) Non-Pay	\$-7,591
Decrease due to a reduction in the technical debt funding profile following completion of several technical refresh initiatives. Technical debt funding is being used to invest in hardware, software, and IT infrastructure in FY 2026. Specifically, this funding is purchasing cables and switches that improve Pentagon facilities and support infrastructure modernization. (FY 2026 Baseline: \$518,571 thousand)	
2) Civilian Compensation.....	\$-5,122
\$1,766 thousand decrease to reflect updated Federal Employees Retirement System (FERS) contribution rates driven by changes in actuarial assumptions, workforce demographics, and projected retirement liabilities. These periodic adjustments lower the Department's required contributions for both Revised Annuity Employees (RAE) and Further Revised Annuity Employees). The decrease aligns funding with current long term cost projections while maintaining full support for civilian retirement benefits and ensuring continued compliance with government wide retirement funding requirements.	
\$1,623 thousand, eight FTEs decrease due to a transfer to O&M Cyber for workforce rebalancing. As DISA completes workforce optimization, DISA determined that additional Cyber FTEs are important to mission success and rebalanced its FTEs alignment between Cyber and Non-Cyber. Growing mission requirements	

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

in the areas of Perimeter Defense, Zero Trust, and Identity, Credential, and Access Management necessitate additional FTEs in the Cyber domain.

\$922 thousand decrease to realize anticipated cost savings to executive, general and special schedules and benefits for current employees. DISA anticipates achieving cost savings in Non-Cyber Pay due to the impact of Deferred Resignation Program departures on Non-Cyber workforce composition.

\$811 thousand, four FTEs decrease is due to rightsizing to account for the ongoing impacts of the departures. Since departures extend into FY 2026, DISA expects its FTE levels to decline slightly in FY 2027 before rising to meet DISA's approved Defense Comprehensive Review levels in FY 2028.
(FY 2026 Baseline: \$447,735 thousand; 2,239 FTEs; -12 FTEs)

3) Shared Services Non-Pay\$-17,935
\$11,503 decrease due to decline in allocation for Facilities, Sustainment, Restoration, and Modernization. FY 2026 funding enabled DISA to complete deferred facilities maintenance and address outstanding projects at multiple sites. DISA will address fewer projects using discretionary funding in FY 2027.

\$4,654 thousand decrease due to a reduction in funding for Defense Finance and Accounting Service (DFAS) financial and human resource services. DISA purchases both finance and human resources services from DFAS. Reductions are due to expected efficiencies from 1) transitioning the DISA General Fund to the same accounting system used for DISA Working Capital Fund activities and 2) reduced processing of human resources transactions due to staffing reductions.

\$1,778 thousand due to the realignment of funding for the Global Solutions Management Operations contract from Shared Services to Network DoW Information Network Operations. DISA is consolidating financial management of the Global Solutions Management Operations contract to ensure a unified approach to managing day-to-day delivery support required to operate and defend the DoW Information Network.
(FY 2026 Baseline: \$105,840 thousand)

4) Joint Staff Support Center (JSSC) Non-Pay\$-105
Decrease due to diminished requirements for Information Technology Support Services contract support.
(FY 2026 Baseline: \$17,216 thousand)

5) Pentagon Reservation Maintenance Revolving Fund (PRMRF) Non-Pay\$-3,564
Decrease to Pentagon Reservation Maintenance Revolving Fund Purchases due to reduced requirements to support the Raven Rock Mountain Complex. Details are classified and available upon request.
(FY 2026 Baseline: \$35,128 thousand)

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

6) Field Commands and Field Offices Non-Pay\$-12,601

\$8,331 thousand decrease due to realignment of funding for the Global Solutions Management Operations contract and other network operations from Field Commands and Field Offices to Network DoW Information Network Operations. DISA is consolidating financial management of the Global Solutions Management Operations contract and other network operations to ensure a unified approach to managing day-to-day delivery support required to operate and defend the DoW Information Network. Global Solutions Management Operations provides subject matter expertise for the development, operations, and sustainment of network capabilities across the DoW in cyber, data, and information mission areas at the DoW Information Network and Warfighter levels. Global Solutions Management Operations ensures that the DoW has the right people and processes in place to manage its global network effectively.

\$4,270 thousand decrease due to efficiencies gained from effective alignment and integration of voice, video, and data services across the Joint Cyber Warfighting Architecture, resulting in diminished sustainment costs. (FY 2026 Baseline: \$45,911 thousand)

7) DoWIN Engineering Services Non-Pay\$-12,871

Decrease due to the reduced requirement for NIPRNet and SIPRNet sensors that support operations, defense and resiliency in support of DoW and Combatant Command (CCMD) Operations with a focus on the European Theatre. (FY 2026 Baseline: \$149,294 thousand)

8) Fourth Estate Network Operations Non-Pay\$-108,868

Decrease due to the planned completion of Defense and Field Activities (DAFAs) onboarding to DoDNet, supported by FY 2026 funds. Sustainment support to DAFAs is significantly less expensive than the initial planning, design, and migration efforts. Migrating DAFAs to DoDNet is a key element of the DoW Zero Trust initiative. Migration provides Zero Trust protection through DISA's Thunderdome program (funded in the DISA Cyber OP-5) upon migration. (FY 2026 Baseline: \$145,667 thousand)

FY 2027 Budget Request\$3,873,222

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

IV. Performance Criteria and Evaluation Summary:

Metric Description	2025 Actuals	2026 Plan	2027 Plan
<u>Department of War Information Network Engineering Services (DoWIN ES):</u>			
1. Percentage of spare capacity maintained to allow for provisioning of unforeseen requirements and rerouting under outages (minimum 25 percent).	1. ≥ 25%	1. ≥ 25%	1. ≥ 25%
2. Number of technical studies of future architectures and enterprise services evaluated for acquisition or technical refresh decisions.	2. 4	2. 4	2. 4
3. Number of Microsoft Defender licenses. Provides secure and compliant software access for end users, enhancing productivity and data protection.	3. 21,000	3. 500,000	3. N/A
4. Number of systems/tools modified/enhanced to modernize DISA's cybersecurity and network architecture to accommodate a Zero Trust Environment.	4. 12	4. 8	4. 4
5. Number of Defense Information Systems Network (DISN) Secret Internet Protocol Router Network (SIPRNet) and Non-Classified Internet Protocol Router Network (NIPRNet) boundary points with monitoring capabilities to ensure consistent performance across key network points.	5. 14	5. 14	5. 14
<u>Data-Centric Enterprise Services (DCES):</u>			
6. Percentage of endpoints protected across DISA classified systems. Endpoints are protected when Data Loss Prevention (DLP) migrations are completed.	6. 25%	6. 50%	6. 75%
7. Number of Azure Virtual Desktop (AVD) migrations completed. The metric measures the total number of CCMDs, Military Services, and	7. 3	7. 3	7. 3

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
Agencies (CC/S/As) that have migrated to AVD within the classified environment.			
8. Number of SIPRNet migrations completed. The metric measures the total number of CCMDs, Military Services, and Agencies locations migrated or adopted SIPR capabilities to meet DoW CIO zero-trust objectives.	8. 60	8. 60	8. 60
9. Percentage of Australia, United Kingdom, and United States (AUKUS) Working Group members from different countries leveraging a single collaboration solution.	9. 0%	9. 30% from AUS & UK	9. 30% from AUS & UK
10. Number of 365-Joint connections to other IL5 (Impact Level) DoW tenants.	10. 18	10. 21	10. 24
11. Number of mailboxes migrated each day to the Tenant-to-Tenant Defense Enterprise Office Solution (DEOS).	11. 350	11. 300	11. 300
12. Number of military users supported by the change of station data transfer.	12. 0	12. 50,000	12. 50,000
13. Operational Availability of DoW Emergency Services IP Network (D-ESINet) pilot.	13. N/A	13. N/A	13. 100%
<u>DoW Enterprise Cloud Computing Ecosystem:</u>			
14. Number of commercial cloud service providers.	14. 4	14. 4	14. 4
15. Number of Joint Operational Edge (JOE) locations operational.	15. 5	15. 6	15. 6
16. Number of Joint Unmanaged Landing Zones installed at JWCC cloud service providers.	16. N/A	16. N/A	16. 4
17. Number of JOE sites with AI acceleration hardware installed.	17. N/A	17. N/A	17. 6
<u>Defense Information Systems Network (DISN) Enterprise Activities (EA):</u>			

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
18. Percentage of time the NIPRNet access circuit is available.	18. 98.80%	18. 98.50%	18. 98.50%
19. SIPRNet Latency (measurement of network delay) in the Continental United States (in milliseconds).	19. 50	19. ≤ 100	19. ≤ 100
20. Number of Internet Protocol (IP) enabling servers / IT components.	20. 241	20. >220	20. >220
21. Number of sites that utilize the Senior National Leadership Communications (SNLC) Gateway/Enclave.	21. 37	21. 37	21. 42
22. Number of Enhanced Pentagon Capability/Survivable Emergency Conferencing Network - Digitalized (EPC/SECN) sites supported.	22. 4	22. 4	22. 5
23. Number of Airborne, Intelligence, Surveillance & Reconnaissance /Unified Video Dissemination System (AISR/UVDS) hubs supported.	23. 7	23. 7	23. 7
24. Number of AISR/Tactical Relays operational.	24. 58	24. 58	24. 58
25. Number of Proliferated Low Earth Orbit (pLEO) Software-Defined Wide Area Network (SD/WAN) enabled deployable DISN nodes available for deployment to global hot spots.	25. N/A	25. 5	25. 5
26. Number of Defense Red Switch Network (DRSN) sites supported.	26. 43	26. 43	26. 43
27. Number of Defense Regional Clocks (DRC) supporting Critical Time Dissemination (CTD)	27. 46	27. 46	27. 47
28. Number of Timing and Synchronization System Capability (TSSC) supporting Critical Time Dissemination (CTD)	28. 30	28. 30	28. 33
<u>Defense Spectrum Organization (DSO):</u>			
29. Number of Electromagnetic Battle Management-Joint (EMBM-J) iterative releases.	29. 5	29. 4	29. 4

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
30. Operational availability of Global Electromagnetic Spectrum Information System (GEMSIS).	30. 99.7%	30. 99.7%	30. 99.7%
31. Number of Electromagnetic Spectrum (EMS) Functions transitioned to modernized EMS IT environment	31. 0	31. 0	31. 2
<u>DoW Teleport Program:</u>			
32. Number of Teleport sites.	32. 14	32. 16	32. 34
33. Number of successful Joint Management Tool (JMT) sustainment tool sprints.	33. 15	33. 15	33. 15
<u>4th Estate Network Optimization (4ENO):</u>			
34. Number of users operational on DoDNet.	34. 23,772	34. 103,840	34. 167,129
35. Number of Defense Agencies and Field Activities (DAFAs) operational on DoDNet.	35. 4	35. 10	35. 16
36. Number of CCMDs completing planning and design phases (including site surveys) for migration to Combatant Command Network Optimization (CCMDNet).	36. N/A	36. N/A	36. 11
<u>Field Commands and Field Offices:</u>			
37. Percentage of spare capacity maintained to allow for provisioning of unforeseen requirements and rerouting under outages (minimum 25 percent).	37. ≥ 25%	37. ≥ 25%	37. ≥ 25%
38. Number of DISA service support plans, Theater Campaign Plans (TCP), and Operational Plans (OPLANs) reviewed.	38. 31	38. 52	38. 52
39. Number of assessments of threat, vulnerability, and risk to the Combatant Command (CCMD) Theater Critical Assets.	39. 70	39. 70	39. 74

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
40. Number of assessments of Command, Control, Computer, Communication, Intelligence, Surveillance, and Reconnaissance (C4ISR) readiness, service constraints, and delivery.	40. 22	40. 24	40. 22
41. Number of U.S./Indo-Pacific/NATO DISA C4ISR Interoperability Reviews.	41. 8	41. 8	41. 8
<u>Network (DoWIN) Operations (NetOps):</u>			
42. Average number of DISN service interruptions mitigated per month.	42. 26,500	42. 60,000	42. 37,000
43. Average number of malicious DISN cyber events blocked and/or mitigated per month.	43. 940 million	43. 1,000 million	43. 1,100 million
44. Number of DISN NetOps network assets managed.	44. 190 million	44. 190 million	44. 190 million
45. Number of Command and Control (C2) Service Telecommunications Service Orders (TSO) and circuit actions processed.	45. 42,300	45. 49,000	45. 39,000
<u>Joint Staff Support Center (JSSC):</u>			
46. Percentage of incidents resolved. Note: JSSC provides over 250 thousand patches per year for Nuclear Command and Control (NC2) and Command and Control (C2) Systems and 12,000 patches per year for Video, Graphic, Intel, and Video Teleconference (VTC) products. JSSC elevates incidents to the program manager as required.	46. 100%	46. 100%	46. 100%
47. Percentage of IT Support availability for over 1,000 Nuclear Decision Conferences and over 600 Worldwide Global Command and Control System – Joint/Joint Planning and Execution Services (GCCS-J/JPES) sites. Target is to maintain 99 percent global availability of critical sites world-wide and 24x7 monitoring and reporting of and National Military Command Center Command and Control System (NCCS) status, and operational impacts.	47. 100%	47. 100%	47. 100%
<u>Joint Service Provider (JSP):</u>			

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
48. Percentage of asset visibility for compliance through continuous monitoring on the Non-classified Internet Protocol Router Network (NIPRNet).	48. 95%	48. 90%	48. 90%
49. Percentage of credentialed scan rate for every asset (minimum 95 percent). JSP scans every asset once per week.	49. 99%	49. 95%	49. 95%
50. Percentage of data availability for enterprise applications and replicated data for unclassified and classified transport networks (minimum 99 percent).	50. 99%	50. 99%	50. 99%
51. Percentage of availability for all JSP-managed systems and services, including but not limited to Virtual Desktop Infrastructure (VDI), Active Directory, File/Print, and Elastic Sky X (ESX) Infrastructure (minimum 99 percent).	51. 99%	51. 99%	51. 99%
52. Percentage of incident tickets resolved within eight business hours of the incident report (minimum 90 percent).	52. 99%	52. 90%	52. 90%
53. Percentage of time-advanced mission-tolerant infrastructure, systems, and support are available to the Immediate Office of the Secretary of War for a high-availability, workstation-based, computer network. (Critical Infrastructure)	53. 99%	53. 99%	53. 99%
54. Percentage of time communications, Information Technology (IT), and physical security are available to maintain full-scope Information Assurance (IA), Computer Network Defense (CND), and Incident Response (IR). (Security Operations)	54. 99%	54. 99%	54. 99%
55. Percentage of time communications systems and support services to the Immediate Office of the Secretary of War are available. (Communications Support)	55. 99%	55. 99%	55. 99%
56. Percentage of time that SECWARCOMs is available as the single point of contact for all Secretary of War, Immediate Office of Continuity			

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
of Operations/Continuity of Government (COOP/COG) and continuity of the Presidency matters. (COOP/COG)	56. 99%	56. 99%	56. 99%
<u>Joint Planning and Execution Services (JPES):</u>			
57. Operational availability of Joint Operation and Planning Execution System (JOPES). Metric is relevant until the JPES modernization effort is operational, and JOPES is sunset.	57. 100%	57. 100%	57. N/A
58. Operational availability of JPES. Metric is relevant following JPES go-live.	58. N/A	58. 100%	58. 100%
<u>Mission Partner Environment (MPE):</u>			
59. Number of operational Coalition Information Environment nodes.	59. 0	59. 0	59. 5
60. Number of existing MPE capabilities transferred from the Department of the Air Force (DAF) and sustained by DISA.	60. 0	60. 0	60. 3
<u>Shared Services Units/Program Executive Offices:</u>			
61. Percentage of DISA's Data Management Assessments completed. Note: This assessment will help establish a baseline of DoW's maturity level of its overall data program and environment. It is not an inspection or an audit; it is a tool, and the shared understanding derived from the results will enable DoW Chief Data Officer (CDO) to help improve overall data maturity and establish guidance and targets for the Department to achieve the goals of the DoW Data Strategy.	61. 100% Monthly	61. 100% Monthly	61. 100% Monthly
62. Percentage of the DISA Data Catalog (DISA-DC) completed. The DISA-DC is a metadata repository that provides DISA visibility and understanding of its data assets through metadata exposure. The Agency's centralized authoritative repository catalogs business and technical metadata for all DISA data assets.	62. 100% Monthly	62. 100% Monthly	62. 100% Monthly

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
63. Percentage of the DISA Data Catalog connecting to DISA data sources.	63. 100%	63. 100%	63. 100%
64. Percentage of Data Governance Assessments completed.	64. 50%	64. 50%	64. 50%
65. Percentage of DISA data interfaces, data payloads, data dictionaries, and Application Program Interface (API) versions registered in the DISA Data Catalog.	65. 25%	65. 100%	65. 100%
66. Percentage of declassification reviews and required determinations completed for all referrals for equity within a 60-day period.	66. 100% Quarterly	66. 100% Quarterly	66. 100% Quarterly
67. Percentage of End User Software Licenses (Microsoft, Adobe, etc.) validated to ensure that the user accounts of DISA employees are licensed legally and accurately.	67. 100% Monthly	67. 100% Monthly	67. 100% Monthly
<u>White House Communications Agency (WHCA):</u>			
68. Percentage of Secure Unclassified and Classified Presidential Information Technology Community (PITC) Network uptime availability. This is the uptime availability of all PITC networks in support of the President and Vice President of the United States.	68. 99.99%	68. 99.99%	68. 99.99%
69. Percentage of COOP and COG Facilities' uptime. Network uptime for COOP and COG facilities.	69. 99.99%	69. 99.99%	69. 99.99%
70. Percentage of deployable team requirements met for POTUS, VPOTUS, and FLOTUS events.	70. 99.99%	70. 99.99%	70. 99.99%
<u>White House Situation Support Staff (WHSSS):</u>			
71. Percentage of mission support activities for the White House Situation Room (WHSR) sustained without disruption.	71. 99%	71. 99%	71. 99%
<u>Communications Management Control Activity:</u>			

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

Metric Description	2025 Actuals	2026 Plan	2027 Plan
72. Percentage of time the information and orders dissemination tool is available to the authorized users.	72. 99%	72. 99%	72. 99%

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

V. Personnel Summary:

	<u>FY 2025</u>	<u>FY 2026</u>	<u>FY 2027</u>	<u>Change FY 2025/ FY 2026</u>	<u>Change FY 2026/ FY 2027</u>
Active Military End Strength (E/S) (Total)	1,549	1,754	1,859	205	105
Officer	335	434	450	99	16
Enlisted	1,214	1,320	1,409	106	89
Reserve Drill Strength (E/S) (Total)	15	0	0	-15	0
Officer	1	0	0	-1	0
Enlisted	14	0	0	-14	0
Reservists on Full Time Active Duty (E/S) (Total)	10	10	10	0	0
Officer	10	10	10	0	0
Civilian End Strength (Total)	2,567	2,466	2,592	-101	126
U.S. Direct Hire	2,397	2,261	2,308	-136	47
Total Direct Hire	2,397	2,261	2,308	-136	47
Foreign National Indirect Hire	5	5	5	0	0
Reimbursable Civilians	165	200	279	35	79
Active Military Average Strength (A/S) (Total)	1,549	1,754	1,859	205	105
Officer	335	434	450	99	16
Enlisted	1,214	1,320	1,409	106	89
Reserve Drill Strength (A/S) (Total)	15	0	0	-15	0
Officer	1	0	0	-1	0
Enlisted	14	0	0	-14	0
Reservists on Full Time Active Duty (A/S) (Total)	10	10	10	0	0
Officer	10	10	10	0	0

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

	<u>FY 2025</u>	<u>FY 2026</u>	<u>FY 2027</u>	<u>Change FY 2025/ FY 2026</u>	<u>Change FY 2026/ FY 2027</u>
Civilian FTEs (Total)	2,615	2,442	2,566	-173	124
U.S. Direct Hire	2,477	2,239	2,285	-238	46
Total Direct Hire	2,477	2,239	2,285	-238	46
Foreign National Indirect Hire	5	5	5	0	0
Reimbursable Civilians	133	198	276	65	78
Average Annual Civilian Salary (\$ in thousands)	198.8	199.5	202.4	0.7	2.9
Contractor FTEs (Total)	3,370	4,469	4,862	1,099	393

Personnel Summary Explanations:

FY 2026 - FY 2027 is (+46) FTEs (\$s are in Thousands).

DISA has an overall O&M non-cyber increase of +46 civilian FTEs.

There is an increase of 58 FTEs for critical mission needs. These are new FTEs to support White House Communication Agency as it addresses serious deficiencies in its communications environment, the Critical Time Dissemination Program, and the Mission Partner Environment (transfer from Department of the Air Force to DISA).

Decrease of -12 FTEs reflects workforce re-balancing. As part of rebalancing, eight FTEs are transferring to cyber and four are being eliminated. DISA continues to reevaluate its workforce to deploy personnel the most mission sensitive areas and achieve cost-savings through prudent utilization of FTEs.

Post-Departure Workforce Rebalancing (-12 FTEs, -8 transfer to Cyber and -4 overall decrease):

- +15 FTEs to DISN EA
- +12 FTEs to Network DoW Information Network Operations
- +6 FTEs to Field Commands and Field Offices
- +4 FTEs to Joint Planning and Execution Services
- +4 FTEs to Data-Centric Enterprise Services
- +3 FTEs to Global Command and Control System - Joint
- +2 FTEs to DoW Cloud Computing Enterprise

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

+2 FTEs to White House Situation Support Staff
+1 FTE to Communication Management Control Activity
+1 FTE to Senior Leadership Enterprise
-1 FTE from Defense Spectrum Organization
-2 FTEs from DoW Teleport Program
-3 FTEs from Joint Service Provider
-3 FTEs from Combined Advanced Applications
-3 FTEs from Management Headquarters
-8 FTEs from Joint Staff Support Center
-10 FTEs from Shared Services
-32 FTEs from DoW Information Network Engineering Services

Increases for Critical Missions (+58 FTEs):

+40 FTEs to WHCA (includes 10 FTEs for the White House Military Office of Technology)
+9 FTEs to DISN EA
+9 FTEs to Mission Partner Environment (transfer from Department of the Air Force)

FY 2025 - FY 2026 is (-238) FTEs (\$s are in Thousands).

The DISA has an overall decrease of -238 civilian FTEs to optimize the workforce in compliance with Executive Order 14210, "Implementing the President's Department of Government Efficiency Workforce Optimization Initiative."

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

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

	FY 2025 Program	Change from FY 2025 to FY 2026		FY 2026 Program	Change from FY 2026 to FY 2027		FY 2027 Program
		Price Growth	Program Growth		Price Growth	Program Growth	
101 EXEC, GEN'L & SPEC SCHEDULES	493,512	6,315	-52,092	447,735	1,237	14,496	463,468
0199 TOTAL CIVILIAN PERSONNEL COMPENSATION	493,512	6,315	-52,092	447,735	1,237	14,496	463,468
308 TRAVEL OF PERSONS	36,561	913	4,105	41,579	873	-729	41,723
0399 TOTAL TRAVEL	36,561	913	4,105	41,579	873	-729	41,723
647 DISA ENTERPRISE COMPUTING CENTERS	123,048	2,462	-125,374	136	-5	75,085	75,216
671 DISA DISN SUBSCRIPTION SERVICES (DSS)	68,739	-5,498	-37,805	25,436	0	44,007	69,443
672 PRMRF PURCHASES	32,317	-2,085	4,896	35,128	807	-3,564	32,371
677 DISA TELECOMM SVCS - REIMBURSABLE DFAS FINANCIAL OPERATION (OTHER DEFENSE AGENCIES)	94,940	48	-26,715	68,273	-799	83,187	150,661
0699 TOTAL OTHER FUND PURCHASES	332,095	-5,918	-181,161	145,016	783	193,591	339,390
771 COMMERCIAL TRANSPORT	4,992	126	-145	4,973	104	-249	4,828
0799 TOTAL TRANSPORTATION	4,992	126	-145	4,973	104	-249	4,828
912 RENTAL PAYMENTS TO GSA (SLUC)	5,061	126	10,779	15,966	335	-903	15,398
913 PURCHASED UTILITIES (NON-FUND)	7,620	191	-3,503	4,308	90	1,529	5,927
914 PURCHASED COMMUNICATIONS (NON-FUND)	152,950	3,824	-131,316	25,458	535	301,764	327,757
915 RENTS (NON-GSA)	5,743	143	-5,327	559	12	325	896
917 POSTAL SERVICES (U.S.P.S)	3	0	233	236	5	-147	94
920 SUPPLIES & MATERIALS (NON-FUND)	3,082	76	2,513	5,671	119	-2,123	3,667
921 PRINTING & REPRODUCTION	5,479	137	-5,485	131	3	-41	93
922 EQUIPMENT MAINTENANCE BY CONTRACT	1,276,333	31,908	586,012	1,894,253	39,779	372,763	2,306,795
923 FACILITIES SUST, REST, & MOD BY CONTRACT	24,479	612	6,855	31,946	671	-10,978	21,639
925 EQUIPMENT PURCHASES (NON-FUND)	180,707	4,517	-48,302	136,922	2,875	74,540	214,337
932 MGT PROF SUPPORT SVCS	2,068	51	-2,119	0	0	0	0
933 STUDIES, ANALYSIS & EVAL	651	16	-667	0	0	0	0
934 ENGINEERING & TECH SVCS	4,501	112	-4,613	0	0	0	0

**Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2027 Budget Estimates**

	FY 2025 <u>Program</u>	<u>Change from FY 2025 to FY 2026</u>		FY 2026 <u>Program</u>	<u>Change from FY 2026 to FY 2027</u>		FY 2027 <u>Program</u>	
		<u>Price Growth</u>	<u>Program Growth</u>		<u>Price Growth</u>	<u>Program Growth</u>		
937	LOCALLY PURCHASED FUEL (NON-FUND)	51	0	-51	0	0	5	5
957	OTHER COSTS (LAND AND STRUCTURES) OTHER COSTS (SUBSISTENCE AND SUPPORT OF PERSONS)	3,214	80	-3,294	0	0	563	563
964		293	7	-295	5	0	-5	0
987	OTHER INTRA-GOVT PURCH	42,695	1,065	61,600	105,360	2,213	2,536	110,109
989	OTHER SERVICES	53,546	1,338	40,563	95,447	2,004	-80,918	16,533
0999	TOTAL OTHER PURCHASES	1,768,476	44,203	503,583	2,316,262	48,641	658,910	3,023,813
9999	GRAND TOTAL	2,635,636	45,639	274,290	2,955,565	51,638	866,019	3,873,222

Several of the changes on the Defense Information Systems Agency's OP-32 from FY 2026 to FY 2027 represent reclassifications of existing costs rather than program growth. True non-pay program growth is concentrated on Line 922 Equipment Maintenance by Contract.

- The increase on Line 647 DISA Enterprise Computing Centers, Line 671 DISA Defense Information Systems Network Subscription Services, and Line 677 DISA Telecommunication Services - Reimbursable represents reclassifications from Line 914 Purchased Communications (non-fund) and Line 922 Equipment Maintenance by Contract. These changes were made to properly classify the Defense Information Systems Agency's purchases of its working capital fund services and bring classification in line with execution.
- The increase on Line 914 Purchased Communications (non-fund) represents reclassifications from Line 922 Equipment Maintenance by Contract for Defense Information Systems Network Enterprise Activities (Transport) and Line 989 Other Services for White House Communications Agency requirements.
- The increase on Line 922 Equipment Maintenance by Contract is true program growth offset by the reclassifications to Line 647 DISA Enterprise Computing Centers, Line 671 DISA Defense Information Systems Network Subscription Services, Line 677 DISA Telecommunication Services – Reimbursable, and Line 914 Purchased Communications (non-fund).
- The decrease on Line 989 Other Services represents a reclassification to Line 914 Purchased Communications (non-fund) for the White House Communications Agency.