Fiscal Year 2025 Budget Estimates

Defense Information Systems Agency Cyber

March 2024

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

	FY 2023 Actuals	Price Change	Program Change	FY 2024 Estimate	Price Change	Program Change	FY 2025 Estimate
DISA Cyber	658,933	16,335	-148,375	526,893	11,470	-33,467	504,896

- FY 2023 includes $3,211 thousand in Overseas Operations Costs (OOC) Actuals. FY 2024 includes $0 in OOC Estimate. FY2025 includes $0 for the OOC Budget Estimate. OOC were financed previously with former Overseas Contingency Operations (OCO) funding.
- This DoD component is a budget line item in the Operation and Maintenance Defense-wide account and therefore, the FY 2024 Estimate does not reflect a CR adjustment. The overall Operation and Maintenance, Defense-wide account CR adjustment for FY 2024 may be found in the O-1 document.

I. Description of Operations Financed:

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

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

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

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

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

Leverage Data as A Center of Gravity – As the DoD embraces several data-management initiatives, the DISA seek to build a culture that values data as a strategic asset to drive mission effectiveness. When thoughtfully collected and analyzed, data can accelerate innovation and improve service delivery. There is also an inherent power in owning data to control the high ground. The DISA's Chief Data Officer (CDO) will drive the agency toward a more data-centric culture and ensure that data is discoverable, accessible and decision-enabling through secure and modernized systems, standards, and governance. In 2022, the DISA unveiled a plan to improve the DISA's data utilization and integration, network and information technology capabilities and advance its capacity to use data as a strategic asset in accordance with the agency's strategic plan for fiscal years 2022 through 2025. The DISA Data Strategy Implementation Plan will guide how the DISA will manage and exploit data as a critical asset to deliver agile digital capabilities to the nation's warfighter and achieve information dominance.

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

Empower the Workforce – The DISA is a highly complex global organization, composed of military, civilian and government contractor personnel. The DISA recognize the importance of empowering and cultivating an innovative and diverse workforce through a framework that assures accountability, transparency and integrity with military and civilian talent leading within every level of the organization. At the DISA, talent diversification is an important approach towards the different perspectives to enhance problem solving, innovation and service delivery. Our agency is focused on establishing a talent pipeline of high-caliber candidates to serve as the next generation cyber workforce. Workforce 2025 Plan is the DISA's human capital investment to empower and posture the agency's global workforce to better meet the challenges posed by what the 2022 National Defense Strategy calls the "most consequential strategic competitor for the coming decades." Through the Workforce 2025, the DISA will continue to offer professional, leadership and personal growth opportunities to fully develop and retain highly motivated and qualified employees across the agency in support of the warfighter. The DISA recognize the positive impact that a well trained and equipped workforce has on organizational climate and morale and will focus on developing the next generation of leaders throughout the agency.

COVID-19 has brought unprecedented challenges to the DISA and rapidly increased mobile computing needs. With the Department's adoption of hybrid workplace model as it transitioned into a post COVID-19 work environment, the DISA has enabled and is continuing to enhance remote capabilities by accelerating the DoD Mobility Classified Capability and increasing non-classified Internet protocol router network circuit capacity. The DISA enabled mission-critical access to classified capabilities by expanding the ability to support secure remote access and provisioning a range of devices to support users globally. The DISA increased capacity for enterprise services such as the DoD365 video service, outlook web access, and enterprise audio conferencing bridges in order to support the growth of teleworking by five to ten times more. The DISA will continue to make mobility a priority to make secure data access possible from any location.

To be effective in the current world environment, there must also be comprehensive and integrated cyber protection for this infrastructure. The DoD’s long-term cyber strategic approach is based on mutually reinforcing lines of effort to build a more lethal joint force, compete and deter in cyberspace, expand alliances and partnerships, reform the department, and cultivate talent. The current cyber domain is a dynamic, complex, and contested battlespace constantly under attack by an ever-evolving array of highly competent adversaries. These malicious actors seek to leverage the characteristics of the cyber domain to their advantage and compromise our ability to operate effectively in cyberspace. In order to defend against these evolving threats, the DISA is pursuing actions across domains and transport layers that will enhance, standardize, and centralize the defense of our cybersecurity environment. The DISA wants to enhance the defensive architecture with a focus on defending against both external and internal attacks, detecting lateral movement, and fully incorporating a more robust Zero Trust Architecture in a synchronized and standardized defensive implementation.

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

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

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

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

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

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

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

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

The CAM is the tool which the DISA uses to allocate its shared services across the agency's portfolio of programs and component organizations on an evaluated basis and approved by the Office of Chief Financial Officer/Comptroller (OCFO). Examples of costs being allocated includes items such as utilities and building operations at the DISA complex, Fort Meade, MD; the Defense Finance and Accounting Services (DFAS) personnel support. The CAM tool organizes the DISA programs and component organizations into two categories to which specific costs are applicable: The agency-wide costs and the DISA Headquarter (HQ) only cost. For example, activities outside of the Fort Meade complex -- such as the Joint Interoperability Test Command (JITC) -- are not charged a share of the utilities and building operations at the DISA complex, Fort Meade, MD, though they are charged a share of the DFAS personnel support. The United States Strategic Command (USSTRATCOM) Field Office, which is not at Fort Meade and gets its IT support from USSTRATCOM, would only be charged a share of the DFAS personnel support costs. Costs are allocated on the basis of validated measures, like the total number of the DISA billets or the number of the DISA Headquarter personnel. These costs are allocated across both the appropriate general fund and the DWCF activities.

Mission Area: Cyberspace Activities (FY 2025: $ 504,896 thousand)

1. Information Systems Security Program (ISSP)/ Joint Information Environment (JIE) (FY 2025: $499,010 thousand): The ISSP/JIE mission focuses on delivering DoD-wide enterprise solutions to the Combatant Commands (CCMDs) and the DoD components ensuring critical mission execution in the face of cyber-attacks. The program provides solutions to harden the network by:

- Reducing the exposed attack surface and gaps that allow adversaries to exploit and disrupt communications. Critical efforts include deployment and operation of defenses at the perimeter that sit at the boundary between the DoD and the internet protecting over 5 million users with state-of-the-art measures mitigating malicious activities such as viruses, exfiltration, and emergent cyber threats.
- Deploying a secure protocol decryption and re-encryption mechanism to protect communications across the Joint Information Environment (JIE) and through theInternet Access Points (IAPs).
- Provides vital situational awareness to senior decision-makers and network defenders that enable attack detection and diagnosis.
- Supporting safe sharing of information with allies and mission partners, by expanding enterprise services that enables secure access and transfer of data between networks of differing classification levels. The DISA will drive anonymity out of the networks by utilizing cyber identity credentials and expanding this capability on Secret Internet Protocol Router Network (SIPRNet).
- Publishing security guidelines and assessing compliance. The DISA is changing the security technical implementation guides to better enable automation of the DoD's configuration management and reporting processes.
- Enables authentication of the user and device, end-to-end encryption, micro-segmentation of traffic, and dynamic networking, while also providing enhanced cyber situational awareness solution with end-to-end visibility, monitoring, and automation.
- Removes redundant Information Assurance (IA) protections; leverages enterprise defensive capabilities with standardized security suites; protects the enclavesafter the separation of server and user assets; and provides the tool sets necessary to monitor and control all security mechanisms throughout the DoD's JIE.

- Provide oversight of IA programs, projects, and initiatives from requirements management though implementation and sustainment.
- Providing training to the DoD civilians by continuing to generate information assurance and NetOps training used throughout the Department using web enabledtools.
- The JRSS is a joint DoD security architecture comprised of complementary defensive security solutions. JRSS provides network security for over 1.7 million users across the Military Departments.
- The Thunderdome is DISA's initial implementation of a Zero Trust Architecture (ZTA) (under the concept of least privileged access). Zero-Trust is a data centric security model that eliminates the idea of trusted or untrusted networks, devices, personas, or processes and shifts to multi- attribute-based confidence levels that enable authentication and authorization policies under the concept of least privileged access.
- DevSecOps Operational Container Scanning (DOCS) provides Continuous Compliance Monitoring (CCM) for all Department of Defense (DoD) mission partners containerized applications which cover all the DevSecOps pillars. It also provides Security Technical Implementation Guide (STIG) automation via Compliance as Code files: automated STIG compliance monitoring for popular software technologies.

2. <u>Defense Industrial Base (DIB) (FY 2025: $5,886 thousand)</u>: The DISA, in concert with the Defense Industrial Base Cyber Security Task Force (DIBCS), is a critical enabler in securing the DoD data on the DIB networks and information systems. The DISA is instrumental in providing Information Assurance and Computer Network Defense (IA/CND), support to the DIB through rapid dissemination of cyber threat, vulnerability, and analysis information. This initiative supports the USCYBERCOM operations, intelligence, and analysis devoted exclusively to cyber indications and warning, intrusion detection, incident analysis, incident response, information sharing/knowledge management, and planning. Additionally, this initiative provides critical system enhancements and new USCYBERCOM personnel at the DoD-DIB Collaboration Information Sharing Environment (DCISE), establishing information sharing between the two organizations to promote synergy and streamline operations.

II. Force Structure Summary:

N/A.

III. Financial Summary ($ in Thousands):

		FY 2024				
			Congressional Action			
A. BA Subactivities	**FY 2023 Actuals**	**Budget Request**	**Amount**	**Percent**	**Current Estimate**	**FY 2025 Estimate**
Defense Industrial Base (DIB) - Cyberspace Operations	$6,149	$5,879	$0	0.00%	$5,879	$5,886
Information Systems Security Program (ISSP) / Information Assurance (IA) - Cyberspace Operations	$517,549	$508,777	$0	0.00%	$508,777	$499,010
Network Operations (NetOps)/Joint Force Headquarters DoD Information Network (JFHQ-DODIN) - Cyberspace Operations	$135,235	$0	$0	0.00%	$0	$0
Other Cyber Programs	$0	$12,237	$0	0.00%	$12,237	$0
Total	**$658,933**	**$526,893**	**$0**	**0.00%**	**$526,893**	**$504,896**

III. Financial Summary ($ in Thousands): (Cont.)

B. Reconciliation Summary	**Change FY 2024/FY 2024**	**Change FY 2024/FY 2025**
BASELINE FUNDING	**$526,893**	**$526,893**
Congressional Adjustments (Distributed)	0	
Congressional Adjustments (Undistributed)	0	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
Fact-of-Life Changes (2024 to 2024 Only)	0	
SUBTOTAL BASELINE FUNDING	**526,893**	
Supplemental	0	
Reprogrammings	0	
Price Changes		11,470
Functional Transfers		0
Program Changes		-33,467
CURRENT ESTIMATE	**526,893**	**504,896**
Less: Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$526,893**	**$504,896**

Overseas Operations Costs

Summary of Operation	**FY 2023 Actuals**	**FY 2024 Estimate**	**FY 2025 Estimate**
Operation ENDURING SENTINEL (OES)	$3,211	$0	$0
Operation INHERENT RESOLVE (OIR)	$0	$0	$0
European Deterrence Initiative (EDI)	$0	$0	$0
Other Theater Requirements and Related Missions	$0	$0	$0
Overseas Operations Costs Total	**$3,211**	**$0**	**$0**

III. Financial Summary ($ in Thousands): (Cont.)

FY 2024 President's Budget Request (Amended, if applicable)		**$526,893**
1. Congressional Adjustments		$0
a) Distributed Adjustments	$0	
b) Undistributed Adjustments	$0	
c) Adjustments to Meet Congressional Intent	$0	
d) General Provisions	$0	
2. Supplemental Appropriations		$0
a) Supplemental Funding	$0	
3. Fact-of-Life Changes		$0
a) Functional Transfers	$0	
b) Technical Adjustments	$0	
c) Emergent Requirements	$0	
FY 2024 Baseline Funding		**$526,893**
4. Reprogrammings (Requiring 1415 Actions)		$0
a) Increases	$0	
b) Decreases	$0	

III. Financial Summary ($ in Thousands): (Cont.)

Revised FY 2024 Estimate	**$526,893**
5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings	$0
a) Less: Supplemental Funding	$0
FY 2024 Normalized Current Estimate	**$526,893**
6. Price Change	$11,470
7. Functional Transfers	$0
a) Transfers In	$0
b) Transfers Out	$0
8. Program Increases	$1,761
a) Annualization of New FY 2024 Program	$0
b) One-Time FY 2025 Increases	$0
c) Program Growth in FY 2025	$1,761
1) Civilian Compensation	$1,761

Increase of Funding and +8 Direct FTEs reflects an internal rephasing to support Thunderdome. In the past, the DISA experienced significant over execution in Direct FTEs. As a result, the Agency increase civilian FTE levels in over executing programs in past budgets and gradually rephased these FTEs across future years. The increase of Direct FTEs represents this year's rephasing levels; as well as, to reflect the proper Average Annual Rate (AAR) for the agency.
(FY 2024 Baseline: $50,140 thousand; 239 FTEs; +8 FTEs)

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

9. Program Decreases ....$-35,228

a) Annualization of FY 2024 Program Decreases $0

b) One-Time FY 2024 Increases $0

c) Program Decreases in FY 2025 .... $-35,228

1) Civilian Compensation to O&M Non Cyber .... $-1,639
Decrease of Funding and FTEs reflects an internal realignment of DISA's workforce. The DISA included an agency-wide reconciliation between cyber and non cyber efforts; to better align the budgeted personnel distributions in its budgeting system to the agency's official manpower database. The DISA will continue to evaluate and make necessary adjustments to ensure civilian personnel counts and compensation rates are accurately budgeted and are in alignment with the manpower database.
(FY 2024 Baseline: $50,140 thousand; 239 FTEs; -14 FTEs)

2) ISSP/PKI/IA/JRSS .... $-21,095
The decrease is the result of reduced costs related to planned scaling down of JRSS operational level of efforts to match the planned decommissioning of the JRSS users by FY 2027offset by funding for implementing upgrade enhancements.

Planned scaling down of JRSS operational level of efforts reflects the de-commissioning of hardware /software (HW/SW) assets, scaled down testing, tier III engineering, assessment, and authorization (A&A), and lab requirements, and a reduction in stacks to meet the sunset schedule of JRSS by 2027.

Implementing upgrade enhancements will center around an enterprise gateway solution set for Military Departments (MILDEP), Secret Internet Protocol Router Network (SIPRNet) Releasable Demilitarized (REL DMZ), Federal DMZ (FED DMZ), and Defense Industrial Base (DIB) partners for the SIPRNet domain. DISA will implement Zero Trust Edge (ZTE), Customer Security Stack (CESS), and Software Defined Wide Area Network (SD-WAN) components to support the gateways in enabling micro-segmentation, Identity, Credential, and Access Management (ICAM), and enhanced inspection and visibility of gateway communications through a consolidated Multi-Cloud Impact Level 6 (IL6) Defensive Cyber Operations (DCO) architecture.

IL6 provides storage and processing of classified information. The IL6 licenses upgrades allow for the use of

III. Financial Summary ($ in Thousands): (Cont.)

the complete set of Security Event Information Management (SEIM) tools available from Microsoft, including real-time threat detection and prevention for classified endpoints. IL6 licenses upgrades are for following DoD classified applications and tools: Microsoft Defender for Endpoint, Defender for Identity, Microsoft Defender, Azure Information Protection Plan 2, Attribute Based Access Control, Sensitivity labels for Online Web Apps, Teams, Sentinel, Outlook, SharePoint Online, Power Platform and Basic Graph Application Programming Interface (API) capabilities.
(FY 2024 Baseline: $458,637 thousand)

3) Other Cyber Programs .... $-12,494
The decrease reflects a realignment of cyber funding associated with the Distributed Continuity Integrated Network - Top Secret Enterprise Services (DCIN-TS ES) to non-cyber baseline, consistent with the remaining DCIN-TS funding portfolio.
(FY 2024 Baseline: $12,237 thousand)

FY 2025 Budget Request $504,896

IV. Performance Criteria and Evaluation Summary:

Metric Description	2023 Actuals	2024 Plan	2025 Plan
Information Systems Security Program (ISSP) / Assurance (IA) Public Key Infrastructure (PKI):			
1. Number of User Accounts: Continuous Monitoring and Risk Scoring (CMRS) - How many new user accounts with defined permissions were created in the past 365 days?	1. NIPR 411 SIPR 208	1. NIPR 493 SIPR 250	1. NIPR 592 SIPR 300
2. Number of Classes: Provide onsite engineering expertise; training classes and software licensing/maintenance in support of the User Activity Monitoring (UAM) capability in countering insider threats at ten Combatant Commands (CCMDs) and 11 DAFAs	2. 9 Classes	2. 9 classes	2. 9 Classes
3. Percentage of applications behind the Web Application Firewall (WAF): Objective is to protect 100% of internet Facing, Defense Enterprise Computing Center (DECC) hosted, applications with the Web Application Firewall	3. 72%	3. 90%	3. 90%
4. Ticket Completion Percentage: DoD Cyber Exchange content requests are tracked in a ticketing system and 95% will be completed within the terms of the Service Level Agreement (SLA).	4. 96%	4. 95%	4. 95%
5. Number of cybersecurity awareness training courses: Develop & Update 7 online cybersecurity awareness courses hosted on cyber.mil for DoD use.	5. 7	5. 7	5. 7
6. Average number of tickets per day: Joint Information Management System (JIMS) - Average number of tickets created per day in the last 30 days	6. 37	6. 40	6. 40
7. Number of Analytics developed: Analytics - Develop new analytic or major release to existing analytic	7. 10	7. 15	7. 15
8. Number of DoD applications integrated with the Defense Enterprise Identity, Credential, and Access Management (ICAM) Identity Provider (IdP) and Automated Account Provisioning (AAP): Integrate DoD applications with DISA's Defense Enterprise Identity, Credential, and Access Management (ICAM) service to improve DoDIN security by minimizing account/identity-based vulnerabilities and enforcing standardization	8. IDP 127 AAP 17	8. IDP 130 AAP 34	8. IDP 130 AAP 34
9. Number of DoD Cyber Workforce framework (DCWF) training courses: Develop & Update 9 student self-paced cyber training courses mapped to the DoD Cyber Workforce framework (DCWF)	9. 9	9. 9	9. 9

IV. Performance Criteria and Evaluation Summary:

Metric Description	2023 Actuals	2024 Plan	2025 Plan
Thunderdome:			
10. Number of Migrations: Completed Thunderdome Migrations	10. 13 Migrations	10. 60 Migrations	10. 80 Migrations
Cloud Support:			
11. DoD Provisional Authorizations: Number of DoD Provisional Authorizations (PAs) issued based on DoD Assessment (non-reciprocity).	11. 60	11. 85	11. 105
12. Annual Assessments: Complete annual assessments of DoD authorized Cloud Service Provider/Cloud Service Offerings.	12. 60	12. 85	12. 105
13. Receive and review monthly Continuous Monitoring reports and file in secure repository. Resolve problems that are identified: DoD Continuous Monitoring (Continuous Monitoring) reports reviewed, resolved and filed.	13. 720	13. 1020	13. 1260
Connection Approval Program:			
14. Connection Approval Office: Process up to 650 connection approval packages per month to support Combatant Commands / Services / Agencies / Field Activities (CC/S/A/FA) requirements for Defense Information Systems Network (DISN) connections.	14. 992 monthly	14. 650 monthly	14. 650 monthly
15. Defense Security/Cybersecurity Authorization Working Group: Conduct one Defense Security/Cybersecurity Authorization Working Group (DSAWG) meeting per month to include agenda, minutes, and ballots. Process eVotes as required for those decisions made outside the DSAWG meeting.	15. 3 monthly	15. 3 monthly	15. 3 monthly
16. Cross Domain Solution: Conduct one Cross Domain Technical Advisory Board (CDTAB) meeting per month. Process up to 60 cross domain actions per month including eVotes.	16. 1 monthly	16. 1 monthly	16. 1 monthly
17. Ports Protocols Service Management (PPSM): Conduct one Ports Protocols Service Management (PPSM) Configuration Control Board/Technical Advisory Group (CCB/TAG) per month. Process up to 160 PPSM actions per month as required by Combatant Commands / Services / Agencies / Field Activities (CC/S/A/FA) submissions.	17. 1 monthly	17. 1 monthly	17. 1 monthly
18. Document Review, Computer Based Training (CBT) Development, Cyber SME: Provide 4 document reviews, produce 2 Computer Based Trainings (CBTs), and provide 4 SME analysis per month to support Connection Approval Program requirements.	18. 100%/ Monthly	18. 100%/ Monthly	18. 100%/ Monthly

IV. Performance Criteria and Evaluation Summary:

Metric Description	2023 Actuals	2024 Plan	2025 Plan
19. Register Cloud Service Offerings that have DoD Pas (Impact Level 4, 5 and 6) or Combatant Commands / Services / Agencies / Field Activities / ADD / Authorization to Operate (CC/S/A/FA/ADD/ATOs (Impact Level 2) This metric is keyed off DoD signed Provisional Authorizations. The measured value will be based on the number of Cloud Service Offerings (CSO) entered into the Systems Network Approval Process or Standard Global Services (SGS) Database compared to the number of signed DoD Provisional Authorizations. Cloud Service Offerings (CSO) registrations in Systems Network Approval Process shall take no more than 5 business days. Projected Cloud Service Offerings (CSO) entries is 10 per month. 20. Process Registered Cloud Information Technology IT Projects submitted by Combatant Commands / Services / Agencies / Field Activities (CC/S/A/FA): Process up to 50 Cloud Information Technology (IT) Project connection approval packages per month as required by Combatant Commands / Services / Agencies / Field Activities (CC/S/A/FA) submissions. Insider Threat User Activity Monitoring 21. User Activity Monitoring Implementation: The metric measures the Insider Threat teams implementation status across DISA classified systems. 22. Comprehensive detection program (Committee on National Security Systems Directive 504 Annex b): This metric tracks the implementation of triggers as recommended by 11 categories listed in table 1 of Committee on National Security Systems Directive 504. 6 Categories projected. Security Technical Implementation Guide 23. Update approx. 65 Security Technical Implementation Guides QTR: Security Technical Implementation Guide updates are determined at the pre-release meeting held each quarter. The updates are determined by trouble tickets, patch updates, policy changes, and are prioritized by the government. 24. Respond to trouble tickets (Security Technical Implementation Guide): Estimated 200 per quarter. 25. Vendor Security Technical Implementation Guides: Number of vendor-developed STIGs developed and published.	19. 100%/ Monthly 20. 100%/ Monthly 21. 18/24 22. 99/132 23. 298 24. 905	19. 100%/ Monthly 20. 100%/ Monthly 21. 24 22. 132 23. 260 24. 804	19. 100%/ Monthly 20. 100%/ Monthly 21. 24 22. 132 23. 260 24. 804

IV. Performance Criteria and Evaluation Summary:

Metric Description	2023 Actuals	2024 Plan	2025 Plan
26. Update Security Technical Implementation Guides: Number of updates to existing Windows STIGs developed and published. 27. Benchmark Development Quarterly: Automated benchmarks normally delivered with quarterly release. 28. Compliance and Enforcement: Automated remediation tools. 5 Per year	25. 17 26. 1 27. 54 28. 6	25. 24 26. 3 27. 68 28. 5	25. 20 26. 2 27. 68 28. 5

V. Personnel Summary:

	FY 2023	FY 2024	FY 2025	Change FY 2023/ FY 2024	Change FY 2024/ FY 2025
Active Military End Strength (E/S) (Total)	**99**	**107**	**107**	**8**	**0**
Officer	44	44	44	0	0
Enlisted	55	63	63	8	0
Civilian End Strength (Total)	**361**	**251**	**247**	**-110**	**-4**
U.S. Direct Hire	361	251	247	-110	-4
Total Direct Hire	**361**	**251**	**247**	**-110**	**-4**
Active Military Average Strength (A/S) (Total)	**99**	**107**	**107**	**8**	**0**
Officer	44	44	44	0	0
Enlisted	55	63	63	8	0
Civilian FTEs (Total)	**344**	**239**	**235**	**-105**	**-4**
U.S. Direct Hire	344	239	235	-105	-4
Total Direct Hire	**344**	**239**	**235**	**-105**	**-4**
Average Annual Civilian Salary ($ in thousands)	**187.7**	**209.8**	**220.1**	**22.1**	**10.3**
Contractor FTEs (Total)	**694**	**777**	**773**	**83**	**-4**

Personnel Summary Explanations:
FY 2024 - FY 2025 is (-4) FTEs. The FTE change is due to the following:

1. Increase of +8 Direct FTEs reflects an internal rephasing. In the past, the DISA experienced significant over execution in Direct FTEs. As a result, the Agency increase civilian FTE levels in over executing programs in past budgets and gradually rephased these FTEs across future years. The increase of Direct FTEs represents this year's rephasing levels; as well as, to reflect the proper Average Annual Rate (AAR) for the agency.

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

2. Decrease of -14 FTEs reflects an internal realignment of DISA’s workforce. The DISA included an agency-wide reconciliation between cyber and non cyber efforts; to better align the budgeted personnel distributions in its budgeting system to the agency’s official manpower database. The DISA will continue to evaluate and make necessary adjustments to ensure civilian personnel counts and compensation rates are accurately budgeted and are in alignment with the manpower database.

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

			Change from FY 2023 to FY 2024			Change from FY 2024 to FY 2025		
		FY 2023 Program	Price Growth	Program Growth	FY 2024 Program	Price Growth	Program Growth	FY 2025 Program
101	EXEC, GEN'L & SPEC SCHEDS	64,553	3,246	-17,659	50,140	1,458	122	51,720
0199	**TOTAL CIVILIAN PERSONNEL COMPENSATION**	**64,553**	**3,246**	**-17,659**	**50,140**	**1,458**	**122**	**51,720**
308	TRAVEL OF PERSONS	2,271	50	-2,097	224	5	-3	226
0399	**TOTAL TRAVEL**	**2,271**	**50**	**-2,097**	**224**	**5**	**-3**	**226**
672	PRMRF PURCHASES	110	16	-126	0	0	0	0
0699	**TOTAL OTHER FUND PURCHASES**	**110**	**16**	**-126**	**0**	**0**	**0**	**0**
771	COMMERCIAL TRANSPORT	72	1	-73	0	0	0	0
0799	**TOTAL TRANSPORTATION**	**72**	**1**	**-73**	**0**	**0**	**0**	**0**
914	PURCHASED COMMUNICATIONS (NON-FUND)	89,823	1,976	-91,673	126	3	-2	127
920	SUPPLIES & MATERIALS (NON-FUND)	95	2	90	187	4	-3	188
922	EQUIPMENT MAINTENANCE BY CONTRACT	442,642	9,738	16,390	468,770	9,844	-33,383	445,231
923	FACILITIES SUST, REST, & MOD BY CONTRACT	1,518	33	-1,551	0	0	0	0
925	EQUIPMENT PURCHASES (NON-FUND)	5,911	130	-5,805	236	5	-1	240
932	MGT PROF SUPPORT SVCS	13,032	287	-13,319	0	0	0	0
934	ENGINEERING & TECH SVCS	38,395	845	-39,240	0	0	0	0
987	OTHER INTRA-GOVT PURCH	194	4	-192	6	0	1	7
989	OTHER SERVICES	317	7	6,880	7,204	151	-198	7,157
0999	**TOTAL OTHER PURCHASES**	**591,927**	**13,022**	**-128,420**	**476,529**	**10,007**	**-33,586**	**452,950**
9999	**GRAND TOTAL**	**658,933**	**16,335**	**-148,375**	**526,893**	**11,470**	**-33,467**	**504,896**