Fiscal Year 2024 Budget Estimates

Defense Information Systems Agency Cyber

March 2023

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

	FY 2022* Actuals	Price Change	Program Change	FY 2023 Enacted	Price Change	Program Change	FY 2024** Estimate
DISA Cyber	612,560	14,337	31,746	658,643	16,721	-148,471	526,893

I. Description of Operations Financed:

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

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

I. Description of Operations Financed: (Cont.)
in this area comes through partnerships with industry and academia, and the use of innovative acquisition strategies.

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

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

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

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

To be effective in the current world environment, there must also be comprehensive and integrated cyber protection for this infrastructure. The

I. Description of Operations Financed: (Cont.)

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 byan 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 theDISA 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 sharedservices, and addresses efficiencies.

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

I. Description of Operations Financed: (Cont.)

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

Mission Area: Cyberspace Activities (FY 2024: $ 526,893 thousand)

1. Information Systems Security Program (ISSP)/ Joint Information Environment (JIE) (FY 2024: $508,777 thousand): The ISSP/JIE mission focuses on delivering DoD-wide enterprise solutions to the Combatant Commands (COCOMS) 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

I. Description of Operations Financed: (Cont.)

all security mechanisms throughout the DoD's Joint Information Environment. The Joint Regional Security Stack (JRSS) is a joint DoD security architecture comprised of complementary defensive security solutions.

- 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 Thunderdome prototype 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.

2. Defense Industrial Base (DIB) (FY 2024: $5,879 thousand): The DISA, in concert with the Defense Industrial Base Cyber Security Task Force (DIBCS), is acritical 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. Detailed information is submitted separately in classified DoD exhibits.

3. Other Cyber Programs (FY 2024: $12,237 thousand): This program/mission is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.

II. Force Structure Summary:
N/A

III. Financial Summary ($ in Thousands):

		FY 2023					
			Congressional Action				
A. BA Subactivities	**FY 2022* Actuals**	**Budget Request**	**Amount**	**Percent**	**Appropriated**	**Current Enacted**	**FY 2024** Estimate**
Defense Industrial Base (DIB) - Cyberspace Operations	$9,228	$6,162	$0	0.00%	$6,162	$6,162	$5,879
Information Systems Security Program (ISSP) / Information Assurance (IA) - Cyberspace Operations	$447,243	$502,789	$5,000	0.99%	$507,789	$507,789	$508,777
Network Operations (NetOps)/Joint Force Headquarters DoD Information Network (JFHQ-DODIN) - Cyberspace Operations	$156,089	$121,763	$10,000	8.21%	$131,763	$131,763	$0
Other Cyber Programs	$0	$12,929	$0	0.00%	$12,929	$12,929	$12,237
Total	**$612,560**	**$643,643**	**$15,000**	**2.33%**	**$658,643**	**$658,643**	**$526,893**

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

B. Reconciliation Summary	Change FY 2023/FY 2023	Change FY 2023/FY 2024
BASELINE FUNDING	**$643,643**	**$658,643**
Congressional Adjustments (Distributed)	15,000	
Congressional Adjustments (Undistributed)	0	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
SUBTOTAL APPROPRIATED AMOUNT	**658,643**	
Fact-of-Life Changes (2023 to 2023 Only)	0	
SUBTOTAL BASELINE FUNDING	**658,643**	
Supplemental	0	
Reprogrammings	0	
Price Changes		16,721
Functional Transfers		-121,763
Program Changes		-26,708
CURRENT ESTIMATE	**658,643**	**526,893**
Less: Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$658,643**	**$526,893**

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

FY 2023 President's Budget Request (Amended, if applicable)	**$643,643**
1. Congressional Adjustments	$15,000
a) Distributed Adjustments	$15,000
1) Program increase - JFHQ-DODIN	$10,000
2) Program increase - UVDS Korea	$5,000
b) Undistributed Adjustments	$0
c) Adjustments to Meet Congressional Intent	$0
d) General Provisions	$0
FY 2023 Appropriated Amount	**$658,643**
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

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

FY 2023 Baseline Funding	**$658,643**
4. Reprogrammings (Requiring 1415 Actions)	$0
a) Increases	$0
b) Decreases	$0
Revised FY 2023 Estimate	**$658,643**
5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings	$0
a) Less: Supplemental Funding	$0
FY 2023 Normalized Current Estimate	**$658,643**
6. Price Change	$16,721
7. Functional Transfers	$-121,763
a) Transfers In	$0
b) Transfers Out	$-121,763
1) JFHQ DoDIN to the U.S. Cyber Command (USCYBERCOM) Decrease reflects the transfer of the JFHQ DoDIN to the U.S. Cyber Command (USCYBERCOM) - The JFHQ–DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses (FY 2023 Baseline: $121,763 thousand; 152 FTEs; -152 FTEs)	$-121,763
8. Program Increases	$58,292

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

a) Annualization of New FY 2023 Program $0

b) One-Time FY 2024 Increases $0

c) Program Growth in FY 2024 ..... $58,292

1) Compensation and Benefits: One additional Compensable Workday $304
One additional compensable day is included in FY2024. The number of compensable days for FY 2023 is 260 days (2,080 hours), and for FY 2024 is 261 days (2,088 hours).
(FY 2023 Baseline: $78,947 thousand)

2) Information Systems Security Program (ISSP)/ Joint Information Environment (JIE) $11,903
Increase is due to resources associated with the Identity Credentialing and Access Management (ICAM) Global Federated User Domain (GFUD) transitioning from non-cyber to cyber to align with Zero-Trust funding and treat ICAM as a single entity. Lastly, the increase for Automated Security Validation (ASV) licensing subscription and the continual implementation of Thunderdome. Thunderdome is the DISA's Zero Trust Architecture which it will provide and integrate with Policy Decision Points (PDPs) that use identity, device, and environment attributes to make user access decisions to resources and workloads at the application layer; move security closer to the customer edge; and enhance visibility and analytics of cloud security to support Defensive Cyber Operations.
(FY 2023 Baseline: $515,718 thousand)

3) Logging Utility for Java (Log4j) $5,155
Increase supports enhancing the security of Log4j in FY24 to address cyber vulnerabilities across the DoD that were identified in Dec 2021 by monitoring, detecting and responding to malicious attacks and installing patches, in accordance with the DISA's mitigation plan.
(FY 2023 Baseline: $520,718 thousand)

4) Zero Trust Architecture $40,930
An Increase of +7 FTEs is for the implementation of Thunderdome, which is the DISA's Zero Trust Architecture. It will provide and integrate with Policy Decision Points (PDPs) that use identity, device, and environment attributes to make user access decisions to resources and workloads at the application layer; move security closer to the customer edge; and, enhance visibility and analytics of cloud security to support Defensive Cyber Operations. Additionally, the increase will implement an enterprise wide Identity, Credential, Access Management (ICAM) capability on both the NIPR and SIPR network fabrics to include the Identity Provider (IdP), Automated Account Provisioning (AAP), and Master User Record

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

(MUR). This will provide the strong identity and workflow automation needed for the Thunderdome Zero Trust solution.
(FY 2023 Baseline: $515,718 thousand; +7 FTEs)

9. Program Decreases ..... $-85,000

a) Annualization of FY 2023 Program Decreases $0

b) One-Time FY 2023 Increases $0

c) Program Decreases in FY 2024 ..... $-85,000

1) Civilian Compensation ..... $-6,170
The decrease reflects an internal realignment of grade structure to reflect the proper Average Annual Rate (AAR) for the agency to ensure mission readiness.
(FY 2023 Baseline: $78,947 thousand; 384 FTEs; +0 FTEs)

2) Enhancement 365 Licensing for Improved Zero Trust ..... $-16,000
Decrease is related to reduced costs from previous Zero Trust investment decisions to offset costs of Microsoft M365 license upgrades for the DoD.
(FY 2023 Baseline: $520,718 thousand)

3) Joint Regional Security Stack (JRSS) ..... $-62,830
Decrease is to sustain the Joint Regional Security Stack (JRSS) and support users currently protected by JRSS on NIPRNet. Supports transfer of funding from Army, Navy & Air Force through FY 27 for shared sustainment cost associated with the JRSS, which provides network security for over 1.7 million users across the Military Departments.
(FY 2023 Baseline: $520,718 thousand)

FY 2024 Budget Request $526,893

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2022 Actual	2023 Plan	2024 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 343 SIPR 165	1. NIPR 472 SIPR 227	1. NIPR 543 SIPR 261
2. Number of Classes: Provide onsite engineering expertise; training classes, hardware warranty and tech refresh, and software licensing/maintenance in support of the User Activity Monitoring (UAM) capability in countering insider threats at ten Combatant Command (COCOMs)	2. 4 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. 60%	3. 75%	3. 95%
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. 98%	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: Average number of tickets created per day in the last 30 days	6. 25	6. 40	6. 45
7. Number of Analytics developed: Analytics - Develop new analytic or major release to existing analytic	7. 17	7. 19	7. 19
8. Number of DoD applications integrated with the Defense Enterprise Identity, Credential, and Access Management (ICAM) service: 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. 83	8. 50	8. 50
9. Number of DoD Cyber Workforce framework 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. 0	9. 9	10. 9
Thunderdome:			
10. Number of Migrations: Competed Thunderdome Migrations	10. N/A	10. 16 Migrations	10. 50 Migrations
Cloud Support:			

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
11. DoD Provisional Authorizations: Number of DoD Provisional Authorizations (PAs) issued based on DoD Assessment (non-reciprocity).	11. 62	11. 16	11. 20
12. Annual Assessments: Complete annual assessments of DoD authorized Cloud Service Provider/Cloud Service Offerings.	12. 20	12. 48	12. 60
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. 719	13. 600	13. 800
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 DISN connections. (Up to 500 packages are under contract)	14. 7353	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. 27	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. 9	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. 8	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%	18. 100%/ Monthly	18. 100%/ Monthly
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	19. 100%	19. 100%/ Monthly	19. 100%/ Monthly

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2022 Actual	2023 Plan	2024 Plan
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 IT Projects submitted by Combatant Commands / Services / Agencies / Field Activities (CC/S/A/FA): Process up to 50 Cloud IT Project connection approval packages per month as required by Combatant Commands / Services / Agencies / Field Activities (CC/S/A/FA) submissions.	20. 100%	20. 100%/ Monthly	20. 100%/ Monthly
Insider Threat User Activity Monitoring			
21. Privileged User Reviews for DISA programs, systems and networks: This metric measures the results of the Information Systems Security Manager quarterly review of their privileged users for the right clearance, need-to-know, roles, and need for continued access quarterly - 4 projected.	21. 9	21. 12	21. 12
22. User Activity Monitoring Implementation: The metric measures the Insider Threat teams implementation status across DISA classified systems. 1 networks projected in FY 2020	22. 18	22. 24	22. 24
23. 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.	23. 99	23. 132	23. 132
Defense Information Systems Network (DISN) ID2 Zero Trust			
24. Survivability of the Department of Defense Information Network due to zero day attacks, misconfigurations, or malicious attacks: Percentage of coverage in the automations / workflows put in place by Zero Trust and Software Defined solutions to increase the survivability and resilience of the network.	24. ≥ 99%	24. ≥ 99%	24. ≥ 99%

V. Personnel Summary:

	FY 2022	FY 2023	FY 2024	Change FY 2022/ FY 2023	Change FY 2023/ FY 2024
Active Military End Strength (E/S) (Total)	**106**	**107**	**107**	**1**	**0**
Officer	63	63	63	0	0
Enlisted	43	44	44	1	0
Civilian End Strength (Total)	**377**	**384**	**239**	**7**	**-145**
U.S. Direct Hire	377	384	239	7	-145
Total Direct Hire	**377**	**384**	**239**	**7**	**-145**
Active Military Average Strength (A/S) (Total)	**106**	**107**	**107**	**1**	**0**
Officer	63	63	63	0	0
Enlisted	43	44	44	1	0
Civilian FTEs (Total)	**377**	**384**	**239**	**7**	**-145**
U.S. Direct Hire	377	384	239	7	-145
Total Direct Hire	**377**	**384**	**239**	**7**	**-145**
Average Annual Civilian Salary ($ in thousands)	**192.5**	**205.6**	**209.8**	**13.1**	**4.2**
Contractor FTEs (Total)	**1,007**	**982**	**995**	**-25**	**13**

Personnel Summary Explanations:
FY 2023 - FY 2024 is (-145) FTEs. The FTE change is due to the following:

A decrease of -152 Direct FTEs reflects the transfer of JFHQ DODIN to the U.S. Cyber Command (USCYBERCOM) - Enhanced Budgetary Control. JFHQ–DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses.

An Increase of +7 FTEs is for the implementation of Thunderdome, which is the DISA's Zero Trust Architecture. It will provide and integrate with Policy Decision Points (PDPs) that use identity, device, and environment attributes to make user access decisions to resources and workloads at

V. Personnel Summary: (Cont.)

the application layer; move security closer to the customer edge; and, enhance visibility and analytics of cloud security to support Defensive Cyber Operations. Additionally, the increase will implement an enterprise wide Identity, Credential, Access Management (ICAM) capability on both the NIPR and SIPR network fabrics to include the Identity Provider (IdP), Automated Account Provisioning (AAP), and Master User Record (MUR). This will provide the strong identity and workflow automation needed for the Thunderdome Zero Trust solution.

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

			Change from FY 2022 to FY 2023			Change from FY 2023 to FY 2024		
		FY 2022* Program	Price Growth	Program Growth	FY 2023 Program	Price Growth	Program Growth	FY 2024** Program
101	EXEC, GEN'L & SPEC SCHEDS	72,566	2,997	3,384	78,947	3,969	-32,776	50,140
0199	**TOTAL CIVILIAN PERSONNEL COMPENSATION**	**72,566**	**2,997**	**3,384**	**78,947**	**3,969**	**-32,776**	**50,140**
308	TRAVEL OF PERSONS	1,272	27	299	1,598	35	-1,409	224
0399	**TOTAL TRAVEL**	**1,272**	**27**	**299**	**1,598**	**35**	**-1,409**	**224**
771	COMMERCIAL TRANSPORT	20	0	-20	0	0	0	0
0799	**TOTAL TRANSPORTATION**	**20**	**0**	**-20**	**0**	**0**	**0**	**0**
914	PURCHASED COMMUNICATIONS (NON-FUND)	115,140	2,418	-116,769	789	17	-680	126
920	SUPPLIES & MATERIALS (NON-FUND)	88	2	427	517	11	-341	187
922	EQUIPMENT MAINTENANCE BY CONTRACT	358,571	7,530	200,477	566,578	12,465	-110,274	468,769
923	FACILITIES SUST, REST, & MOD BY CONTRACT	791	17	-808	0	0	0	0
925	EQUIPMENT PURCHASES (NON-FUND)	28,157	591	-26,647	2,101	46	-1,911	236
934	ENGINEERING & TECH SVCS	26,944	566	-27,510	0	0	0	0
987	OTHER INTRA-GOVT PURCH	0	0	6	6	0	1	7
989	OTHER SERVICES	2,148	45	5,914	8,107	178	-1,081	7,204
990	IT CONTRACT SUPPORT SERVICES	6,863	144	-7,007	0	0	0	0
0999	**TOTAL OTHER PURCHASES**	**538,702**	**11,313**	**28,083**	**578,098**	**12,717**	**-114,286**	**476,529**
9999	**GRAND TOTAL**	**612,560**	**14,337**	**31,746**	**658,643**	**16,721**	**-148,471**	**526,893**

*FY 2022 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).