# Fiscal Year 2023 Budget Estimates

## Defense Information Systems Agency Cyber

April 2022

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

| | FY 2021*<br>Actuals | Price<br>Change | Program<br>Change | FY 2022<br>Enacted | Price<br>Change | Program<br>Change | FY 2023**<br>Request |
|---|---|---|---|---|---|---|---|
| DISA Cyber | 593,553 | 17,334 | -18,509 | 592,378 | 13,912 | 37,353 | 643,643 |

*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).
**The total amount of the FY 2023 request reflects $3,232.0 thousand for Overseas Operations Costs

## 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 three strategic goals:

**Operate and Defend** – In today's landscape of increasing cyber threats, the ability to deliver services and capabilities across all domains – land, air, sea, space, and cyberspace – allows mission partners to maintain global leadership and to deny unwanted advantages to adversaries. The DISA understands these requirements, and its desired end state is to deliver secure, available, and reliable services and capabilities to mission partners in a contested and rapidly changing cyberspace environment. The DISA's support to crisis and combat operations takes on many forms, such as employing tool suites to provide real-time and robust monitoring of an infrastructure to lessen interrupted service or developing interagency and international partnerships to strengthen protection of critical assets. The DISA is on the leading edge of deploying, operating, and sustaining cyber tools, capabilities, and expertise to maximize DoDIN operations that support multi-domain operations and enhance lethality.

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

**Adopt before we buy and buy before we create –** The DISA strives to improve the speed of delivery of services and capabilities for the DoD. When a mission partner requests a solution, the DISA first determines if the solution already exists within the DoD and if it is scalable to meet the mission requirement. Second, if the solution is not available or scalable, the DISA buys it from industry partners. If the solution is not available from the DoD or industry partners, the third and least agile method to fulfill the requirement is by creating a custom solution. This process strengthens mission partner collaboration by developing and delivering acustomized service or capability solution based on the specific requirements while minimizing development costs.

**Enable People and Reform the Agency –** The DISA is a highly complex global organization of military, civilian, and government contractor personnel. The DISA supports many different missions within the Department of Defense and beyond, providing combat support to the warfighters across the globe. To effectively meet these demands, the DISA recognizes the importance of cultivating an innovative and diverse workforce with military and civilian talent within every level of our organization and constantly seeking ways to mature business operations.

**Consistent with the National Defense Strategy -** Charged to reform the Department, the DISA modernizes its infrastructure to improve the security, resiliency, and capacity for the DoD networks. One focus of the DISA's current modernization initiative is to standardize configurations for greater performance and affordability. Another focus is to consolidate and converge data centers, networks, service desks and network operation centers into a secure, integrated, and improved environment. A modern infrastructure reduces the cost and complexity to operate while improving customer service with transparency.

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

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

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

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 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.

**I. Description of Operations Financed: (Cont.)**
**Mission Area: Cyberspace Activities (FY 2023: $643,643 thousand)**

1. Information Systems Security Program (ISSP)/ Joint Information Environment (JIE) (FY 2023: $515,718 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 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

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

processes and shifts to multi- attribute based confidence levels that enable authentication and authorization policies under the concept of least privileged access.

2. Joint Force Headquarters DoD Information Network (JFHQ-DODIN) (FY 2023: $121,763 thousand): The Joint Force Headquarters - DoD Information Networks (JFHQ-DODIN) addresses a critical need for cohesive DoDIN defense and protection and unity of effort within the DoD's existing fragmented cyberspace operations command and control (C2) framework. The JFHQ-DODIN's mission is to exercise command and control of the DoDIN Operations and Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) globally in order to synchronize the protection of the DoD components' capabilities to enable power projection and freedom of action across all warfighting domains. The full mission scope of the JFHQ-DODIN includes: the critical daily requirement to protect the DoDIN, C2 of all the DoD cyber entities, a mature joint headquarters, management of requirements for global engagement, and the capability to assess the readiness of the DoDIN against mission critical Combatant Command requirements.

The (JFHQ-DODIN) provides unity of command between the USCYBERCOM and its subordinate headquarters, unity of effort with all other DoD Components in order to ensure the DoDIN is available and secure for joint missions, to include effects delivered in and through cyberspace, and to ensure that the readiness posture of the DoDIN is known. This organization directs and executes global DoDIN operations and defensive cyber operations. This capability is essential to protecting all of the DoD's IT infrastructure and applications against a growing international cyber threat and an increasing level of insider threats.

3. Defense Industrial Base (DIB) (FY 2023: $6,162 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.

**Fiscal Year (FY) 2023 Overseas Operations Costs funding accounted for in the Base budget include:**

- Operation INHERENT RESOLVE (OIR) [$3,232 thousand].
- Operation European Deterrence Initiative (EDI) [$0 thousand].
- Other theater requirements and related missions [$0 thousand].

## II. Force Structure Summary:

N/A

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

| | | FY 2022 | | | | | |
|---|---|---|---|---|---|---|---|
| | | | Congressional Action | | | | |
| | FY 2021* | Budget | | | | Current | FY 2023** |
| **A. BA Subactivities** | **Actuals** | **Request** | **Amount** | **Percent** | **Appropriated** | **Enacted** | **Request** |
| Defense Industrial Base (DIB) - Cyberspace Operations | $9,250 | $9,795 | $0 | 0.00% | $9,795 | $9,795 | $6,162 |
| Information Systems Security Program (ISSP) / Information Assurance (IA) - Cyberspace Operations | $474,654 | $426,406 | $0 | 0.00% | $426,406 | $426,406 | $515,718 |
| Network Operations (NetOps)/Joint Force Headquarters DoD Information Network (JFHQ-DODIN) - Cyberspace Operations | $109,649 | $94,077 | $62,100 | 66.01% | $156,177 | $156,177 | $121,763 |
| **Total** | **$593,553** | **$530,278** | **$62,100** | **11.71%** | **$592,378** | **$592,378** | **$643,643** |

*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).
*Overseas Operations costs accounted for in the base budget: $3,232 thousand.

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

| B. Reconciliation Summary | Change<br>FY 2022/FY 2022 | Change<br>FY 2022/FY 2023 |
|---|---|---|
| **BASELINE FUNDING** | **$530,278** | **$592,378** |
| Congressional Adjustments (Distributed) | 62,100 | |
| Congressional Adjustments (Undistributed) | 0 | |
| Adjustments to Meet Congressional Intent | 0 | |
| Congressional Adjustments (General Provisions) | 0 | |
| **SUBTOTAL APPROPRIATED AMOUNT** | **592,378** | |
| Fact-of-Life Changes (2022 to 2022 Only) | 0 | |
| **SUBTOTAL BASELINE FUNDING** | **592,378** | |
| Supplemental | 0 | |
| Reprogrammings | 0 | |
| Price Changes | | 13,912 |
| Functional Transfers | | 0 |
| Program Changes | | 37,349 |
| **CURRENT ESTIMATE** | **592,378** | **643,639** |
| Less: Supplemental | 0 | |
| **NORMALIZED CURRENT ESTIMATE** | **$592,378** | **$643,639** |

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

| | | | |
|---|---|---|---|
| **FY 2022 President's Budget Request (Amended, if applicable)** | | | **$530,278** |
| 1. Congressional Adjustments | | | $62,100 |
| a) Distributed Adjustments | | $62,100 | |
| 1) Program Increase - Hardening DoD Networks | $62,100 | | |
| b) Undistributed Adjustments | | $0 | |
| c) Adjustments to Meet Congressional Intent | | $0 | |
| d) General Provisions | | $0 | |
| **FY 2022 Appropriated Amount** | | | **$592,378** |
| 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 2022 Baseline Funding** | | | **$592,378** |
| 4. Reprogrammings (Requiring 1415 Actions) | | | $0 |

**III. <u>Financial Summary ($ in Thousands)</u>: (Cont.)**

a) Increases ........................................ $0

b) Decreases ........................................ $0

**Revised FY 2022 Estimate ........................................ $592,378**

5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings ........................................ $0

a) Less: Supplemental Funding ........................................ $0

**FY 2022 Normalized Current Estimate ........................................ $592,378**

6. Price Change ........................................ $13,912

7. Functional Transfers ........................................ $0

a) Transfers In ........................................ $0

b) Transfers Out ........................................ $0

8. Program Increases ........................................ $156,836

a) Annualization of New FY 2022 Program ........................................ $0

b) One-Time FY 2023 Increases ........................................ $26,000

1) Enhanced Sensing and Mitigation ........................................ $26,000
Increase is to purchase and sustain an automated and continuous scanning capability for the Department of Defense Information Networks (DoDIN) assets that are phasing out in both the public and external capabilities in order to maintain continuous scanning of probable areas to be examined and identify network weaknesses in DoDIN.
(FY 2022 Baseline: $156,177 thousand)

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

c) Program Growth in FY 2023 .......... $130,836

1) Distributed Continuity Integrated Network - Top Secret Enterprise Services (DCIN-TS-ES) Enhancement.. $12,929
Classified.
(FY 2022 Baseline: $426,406 thousand)

2) Distributed Continuity Integrated Network - Zero Trust Implementation .......... $117,330
Increase 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 (MUR). This will provide the strong identity and workflow automation needed for the Thunderdome Zero Trust solution.
(FY 2022 Baseline: $426,406 thousand; 225 FTEs; +7 FTEs)

3) Travel of Persons ..........$577
Increase in travel supports additional inspections and audit assessments by the Joint Forces Headquarters Department of Defense Information Networks (DoDIN) Red team. There is an increase from 70 audits and inspections, to 125 audits and inspections.
(FY 2022 Baseline: $985 thousand)

9. Program Decreases ..........$-119,487

a) Annualization of FY 2022 Program Decreases ..........$0

b) One-Time FY 2022 Increases .......... $-62,100

1) Program Increase - Hardening DoD Networks.......... $-62,100

c) Program Decreases in FY 2023 .......... $-57,387

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

1) Compensation and Benefits – One less Compensable Work Day........................................................................ $-25
One less compensable day in FY 2023. The number of compensable days for FY 2022 is 261 days (2,088 hours), and for FY 2023 is 260 days (2,080 hours).
(FY 2022 Baseline: $72,734 thousand)

2) Defense Industrial Base (DIB)............................................................................................................... $-3,839
Decrease is due to a one-time increase in FY 2022 for engineering support to migrate DIB networks to the cloud environment. Migration will be completed at the end of FY 2022; thus, the surge is no longer required.
(FY 2022 Baseline: $9,795 thousand)

3) Information Systems Security Program (ISSP) / Information Assurance (IA) .............................................. $-11,417
Decrease is attributed to a one-time increase in FY 2022 for the initial Identity & Credential Access Management (ICAM) software licenses. In FY 2022, the initial purchases were more expensive than the recurring maintenance charges across the lifecycle of the program.
(FY 2022 Baseline: $156,177 thousand)

4) Joint Regional Security Stack (JRSS) ..................................................................................................... $-41,740
Decrease to due to a one-time increase in FY 2022 to support the execution of the Services JRSS, in accordance with the approved plan at the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM). The JRSS is a joint DoD security architecture comprised of complementary defensive security solutions, which supports the joint information environment with the tools set necessary to monitor and control all security mechanism.
(FY 2022 Baseline: $426,406 thousand)

5) Overseas Operations Costs accounted for in the Base Budget......................................................................... $-366
Contingency operations and other theater related requirements and related missions previously funded in OCO. Detailed justifications for Overseas Operations program changes are provided in the Operation and Maintenance, Defense-Wide, Volume 1 Part 2 Book.
(FY 2022 Baseline: $3,524 thousand)

**FY 2023 Budget Request.................................................................................................................................................$643,639**

## IV. Performance Criteria and Evaluation Summary:

| Metric Description by Program | 2021 Actual | 2022 Plan | 2023 Plan |
|---|---|---|---|
| Information Systems Security Program (ISSP)/Joint Information Environment (JIE): | | | |
| 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 334<br>SIPR 184 | 1. 360 NIPR<br>300 SIPR | 1. NIPR 425<br>SIPR 275 |
| 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 (CCMDs) | 2. 4 Classes | 2. 4 classes | 2. 4 Classes |
| 3. Number of Releases Per Year: Engineering and integration of two Secure Host Baseline (SHB)/ WIN10 releases per year | 3. 2 Releases | 3. 2 Releases | 3. 2 Releases |
| 4. 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 | 4. 65% | 4. 95% | 4. 100% |
| 5. Number of Courses: Develop and maintain training for cyber role-based training courses linked to DOD Directive-8140 & DoD Cyber Workforce Framework | 5. 30 Courses | 5. 30 Courses | 5. 30 Courses |
| 6. Average number of tickets per day: Average number of tickets created per day in the last 30 days | 6. 18 Tickets | 6. 60 Tickets | 6. 65 Tickets |
| 7. Number of Analytics developed: Analytics - Develop new analytic or major release to existing analytic | 7. 23 Analytics | 7. 19 Analytics | 7. 19 Analytics |
| 8. Raise-the-Bar (RTB) Expansion of Cross Domain Enterprise Service (CDES) Locations: Increase CDES capabilities to OCONUS locations (INDOPACOM AOR Japan and CENTCOM AOR Bahrain) to support RTB requirements. | 8. 0 | 8. N/A | 8. 1 Location |
| 9. Ticket Completion: 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). | 9. 96% | 9. 95% | 9. 95% |
| Mission Support Organization – Chief Information Officer (MSO-CIO): | | | |
| 10. FY20 Declassification Review Metrics: Complete reviews for all referrals for equity within a 60-day period and make the required determinations for each document. | 10. 100% | 10. 100% Quarterly | 10. 100% Quarterly |

## IV. Performance Criteria and Evaluation Summary:

| Metric Description by Program | 2021 Actual | 2022 Plan | 2023 Plan |
|---|---|---|---|
| 11. Organizational Execution Plan (OEP)/Business Enterprise Architecture (BEA)/Business Capability Acquisition Cycle (BCAC): Report status of timely completion/submission – on a quarterly basis – of the DISA CIO OEP portfolio (and any execution-period changes) for the Pre-Certification Authority (number of submissions submitted timely against total number of submission that quarter). | 11. 100% Monthly | 11. 100% Monthly | 11. 100% Monthly |
| Mission Support Organization – Risk Management MSO/RE- Cyber Security Policy/Risk Management | | | |
| 12. Compliance with requested Cross Domain Support: Accurate and timely preparation of Cross Domain packages. | 12. 100% Monthly | 12. 100% Monthly | 12. 100% Monthly |
| 13. Compliance with Federal Information Systems Management Act: Daily monitoring of Cyber Scope Tool and DoD Information Technology Portfolio Repository (DITPR) | 13. 100% Monthly | 13. 100% Monthly | 13. 100% Monthly |
| 14. DISA CIO REC1 reports weekly on 8570 cyber workforce including qualification status (based on DoD Baseline Certification): Periodic inspection of deliverable products and services - 8570 Compliance Team reports the qualification percentages of the Agency's IA workforce on a weekly basis determining if IA positions (civilian, military and contractor support personnel) have the appropriate DoD Baseline Certification to perform their assigned duties | 14. 100% 1st Quarter | 14. 100% Monthly | 14. 100% Monthly |
| 15. Compliance with DISA Whitelist Requests: Accurate and timely preparation of Whitelist packages. | 15. 100% Monthly | 15. 100% Monthly | 15. 100% Monthly |
| 16. Compliance with Communications Tasking Order (CTO) 10-133 waiver Requests: Accurate and timely preparation of CTO 10-133 waiver packages. | 16. 100% Monthly | 16. 100% Monthly | 16. 100% Monthly |
| MSO/RE-Security Technical Implementation Guides (STIGs): | | | |
| 17. Update approx. 65 STIGs QTR: Security Technical Implementation Guides (STIG) 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. | 17. 178 through 3rd Qtr | 17. 260 | 17. 260 |
| 18. Respond to trouble tickets (STIG): Estimated 200 per quarter. | 18. 1336 Through 3rd Qtr | 18. 804 | 18. 804 |
| 19. Vendor STIGS (Target values must be dynamic due to vendor paced): Hycu-Oct, IBM Aspera-Nov, Netapp Ontap-Nov,Vmware Horizonview-Nov, Vmware NSX-Dec, Splunk 8-Dec, Mozilla ESR-Dec, Apple Mac OS 11-Dec, Samsung Android 11-Dec, Forescout-Dec, Crunch Data-Dec,SLES 15-Jan, HPE 3PAR-Jan, Oracle Linux 8- Jan, Redis- Feb, MobileIron Sentry 9.8- Feb, Spec | 19. 8 through 3rd Qtr | 19. 12 | 19. 12 |

## IV. Performance Criteria and Evaluation Summary:

| Metric Description by Program | 2021 Actual | 2022 Plan | 2023 Plan |
|---|---|---|---|
| Innovations- Feb, Rancher Labs-Mar, Nutanix AOS-Mar, Redhat Openshift-Mar, HPE Nimble-Mar, Riverbed Steelcentral Aternity-Apr, MongoDB-May, Dynatrace-June, Cybersecure IMS-June, Arista-July, Hypori-July, Palo Alto Prisma-July, Maria DB-Aug, Redhat Ansible Tower-Aug, Avepoint Compliance Guardian-Aug, Avepoint DocAve-Aug, Avepoint Fly-Aug | | | |
| 20. Develop technology Security Requirements Guides (SRGs) or Protection Profile Annexes: Cloud MO SRG May20. | 20. 3 through 2nd Qtr | 20. 3 | 20. 3 |
| 21. Update STIGs (Estimated completion date): MS Windows May, VMware VSpphere 6.7 Jan | 21. 1 through 2nd Qtr | 21. 3 | 21. 3 |
| 22. Develop new STIGs (Estimated completion dates): InfoBlox 8 Domain Name System (DNS) Dec, Microsoft Edge Jan, CA IDMS Apr, Ubuntu 20.04 Mar,Cisco ASA Mar, Cisco ISE Apr, Citrix Dec, Fortinet Dec,Honeywell Android 9 Jan, IBM Websphere May, Kubernetes Mar, MS O365 May, MS SCOM Feb, Oracle MYSQL 8 Jan, RHEL8 Dec, | 22. 13 through 3rd Qtr | 22. 13 | 22. 13 |
| 23. Benchmark Development Quarterly: Automated benchmarks normally delivered with quarterly release. | 23. 39 through 3rd Qtr | 23. 68 | 23. 68 |
| 24. Compliance and Enforcement: Automated remediation tools. 5 Per year | 24. 3 through 3rd Qtr | 24. 5 | 24. 5 |
| MSO/RE - Connection Approval Program (CAP): | | | |
| 25. Connection approval packages and Cyber Hygiene Analysis: Process up to 650 connection approval packages per month to support CC/S/A/FA requirements for DISN connections. (Up to 500 packages are under contract) | 25. 100% Monthly | 25. 100% Monthly | 25. 100% Monthly |
| 26. Defense Security/Cybersecurity Authorization Working Group (DSAWG): Conduct one DSAWG meeting per month to include agenda, minutes, and ballots. Process eVotes as required for those decisions made outside the DSAWG meeting. | 26. 100% Monthly | 26. 100% Monthly | 26. 100% Monthly |
| 27. 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. | 27. 100% Monthly | 27. 100% Monthly | 27. 100% Monthly |
| 28. Ports Protocols Service Management (PPSM): Conduct one PPSM CCB/TAG per month. Process up to 160 PPSM actions per month as required by CC/S/A/FA submissions. | 28. 100% Monthly | 28. 100% Monthly | 28. 100% Monthly |
| 29. Document Review, Computer Based Training (CBT) Development, Cyber SME: Provide 4 document reviews, produce 2 CBTs, and provide 4 SME analysis per month to support RE4 requirements. | 29. 100% Monthly | 29. 100% Monthly | 29. 100% Monthly |
| | | 30. 100% Monthly | 30. 100% Monthly |

## IV. Performance Criteria and Evaluation Summary:

| Metric Description by Program | 2021 Actual | 2022 Plan | 2023 Plan |
|---|---|---|---|
| 30. Select and Native Programming (SNAP) Registered Cloud Service Offerings: This metric is keyed off DoD signed Provisional Authorizations. The measured value will be based on the number of Cloud Service Offerings entered into the SNAP or SIPRNet GIAP System (SGS) Database compared to the number of signed DoD Provisional Authorizations. Cloud Service Offering (CSO) registrations in SNAP shall take no more than 5 business days. Projected CSO entries is 10 per month | 30. 100% Monthly | | |
| 31. SNAP Registered Cloud IT Projects (Level 4, 5 and 6 only): Process up to 50 Cloud IT Project connection approval packages per month as required by CC/S/A/FA submissions. | 31. 100% Monthly | 31. 100% Monthly | 31. 100% Monthly |
| MSO/RE - Insider Threat User Activity Monitoring: | | | |
| 32. Privileged User Reviews for DISA programs, systems and networks.: This metric measures the results of the ISSM quarterly review of their privileged users for the right clearance, need-to-know, roles, and need for continued access quarterly - 4 projected. | 32. Met through 3rd Qtr | 32. 4 | 32. 4 |
| 33. User Activity Monitoring Implementation: The metric measures the InT teams implementation status across DISA classified systems. 1 network projected in FY20 | 33. Met through 3rd Qtr | 33. 1 | 33. 1 |
| 34. Comprehensive detection program (Committee on National Security Systems Directive CNSSD 504 Annex b): This metric tracks the implementation of triggers as recommended by 11 categories listed in table 1 of CNSSD 504. 6 Categories projected. | 34. Met through 3rd Qtr | 34. 2 | 34. 2 |
| MSO/RE - Cloud Support: | | | |
| 35. DoD Provisional Authorizations: Number of DoD Partner Agencies (PAs) issued based on DoD Assessment (non-reciprocity). | 35. 18 through 3rd Qtr | 35. 12 | 35. 12 |
| 36. Annual Assessments: Complete annual assessments of DoD authorized Cloud Service Provider (CSP) and Cloud Service Offering (CSO) (CSP/CSOs). | 36. 10 through 3rd Qtr | 36. 36 | 36. 36 |
| 37. Receive and review monthly ConMon reports and file in secure repository. Resolve problems that are identified.: DoD Continuous Monitoring (ConMon) reports reviewed, resolved, and filed. | 37. 70 through 3rd Qtr | 37. 144 | 37. 144 |
| Joint Regional Security Stacks (JRSS): | | 38. N/A | 38. N/A |

## IV. Performance Criteria and Evaluation Summary:

| Metric Description by Program | 2021 Actual | 2022 Plan | 2023 Plan |
|---|---|---|---|
| 38. Analytic capability deployment: Implement Joint Management System (JMS) Cyber Situational Awareness Analytic Cloud (CSAAC) analytic capability | 38. 6 | | |
| JFHQ-DODIN Inspections and Audits:<br>39. Number of JFHQ-DODIN Inspection and Audit assessments conducted, and JFHQ-DODIN's ability to direct and certify DoD Inspection forces: JFHQ-DODIN's ability to execute Inspections and Audits to evaluate the strength, cybersecurity posture and resiliency of the DODIN, and ensure the DoD Inspection Workforce is certified and executing as directed | 39. JFHQ-DODIN has executed 84 Inspections and Audits, and the Navy / Army Inspection Workforce has executed 47 Inspections and Audits.  For the month of September, an additional 12 Inspections and Audits are planned. | 39. JFHQ-DODIN executing 125 Inspection and Audits, and the DoD Inspection and Audit Workforce is certified and executing 100 Assessments | 39. JFHQ-DODIN executing 125 Inspection and Audits, and the DoD Inspection and Audit Workforce is certified and executing 100 Assessments |

## V. Personnel Summary:

| | FY 2021 | FY 2022 | FY 2023 | Change FY 2021/ FY 2022 | Change FY 2022/ FY 2023 |
|---|---|---|---|---|---|
| **Active Military End Strength (E/S) (Total)** | **94** | **105** | **106** | **11** | **1** |
| Officer | 56 | 63 | 63 | 7 | 0 |
| Enlisted | 38 | 42 | 43 | 4 | 1 |
| **Civilian End Strength (Total)** | **365** | **377** | **384** | **12** | **7** |
| U.S. Direct Hire | 365 | 377 | 384 | 12 | 7 |
| **Total Direct Hire** | **365** | **377** | **384** | **12** | **7** |
| **Active Military Average Strength (A/S) (Total)** | **94** | **105** | **106** | **11** | **1** |
| Officer | 56 | 63 | 63 | 7 | 0 |
| Enlisted | 38 | 42 | 43 | 4 | 1 |
| **Civilian FTEs (Total)** | **365** | **377** | **384** | **12** | **7** |
| U.S. Direct Hire | 365 | 377 | 384 | 12 | 7 |
| **Total Direct Hire** | **365** | **377** | **384** | **12** | **7** |
| **Average Annual Civilian Salary ($ in thousands)** | **177.9** | **192.9** | **205.6** | **15.0** | **12.7** |
| **Contractor FTEs (Total)** | **1,020** | **1,007** | **982** | **-13** | **-25** |

**Personnel Summary Explanations:**

*Military end strength net increase of +1 enlisted personnel to support out continued force structure growth to provide Cyber support.

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

| | | | Change from FY 2021 to FY 2022 | | | Change from FY 2022 to FY 2023 | | |
|---|---|---|---|---|---|---|---|---|
| | | FY 2021* Program | Price Growth | Program Growth | FY 2022 Program | Price Growth | Program Growth | FY 2023** Program |
| 101 | EXEC, GEN'L & SPEC SCHEDS | 64,654 | 1,468 | 6,612 | 72,734 | 3,000 | 3,213 | 78,947 |
| 106 | BENEFIT TO FMR EMPLOYEES | 202 | 5 | -207 | 0 | 0 | 0 | 0 |
| 121 | PCS BENEFITS | 75 | 2 | -77 | 0 | 0 | 0 | 0 |
| **0199** | **TOTAL CIVILIAN PERSONNEL COMPENSATION** | **64,931** | **1,475** | **6,328** | **72,734** | **3,000** | **3,213** | **78,947** |
| 308 | TRAVEL OF PERSONS | 353 | 11 | 621 | 985 | 21 | 577 | 1,583 |
| **0399** | **TOTAL TRAVEL** | **353** | **11** | **621** | **985** | **21** | **577** | **1,583** |
| 771 | COMMERCIAL TRANSPORT | 17 | 1 | -18 | 0 | 0 | 0 | 0 |
| **0799** | **TOTAL TRANSPORTATION** | **17** | **1** | **-18** | **0** | **0** | **0** | **0** |
| 914 | PURCHASED COMMUNICATIONS (NON-FUND) | 57,174 | 1,715 | -58,122 | 767 | 16 | 1 | 784 |
| 920 | SUPPLIES & MATERIALS (NON-FUND) | 101 | 3 | 381 | 485 | 10 | 10 | 505 |
| 922 | EQUIPMENT MAINTENANCE BY CONTRACT | 454,672 | 13,640 | -5,529 | 462,783 | 9,718 | 79,150 | 551,651 |
| 923 | FACILITIES SUST, REST, & MOD BY CONTRACT | 3,203 | 96 | -3,299 | 0 | 0 | 0 | 0 |
| 925 | EQUIPMENT PURCHASES (NON-FUND) | 9,115 | 273 | 32,057 | 41,445 | 870 | -40,218 | 2,097 |
| 932 | MGT PROF SUPPORT SVCS | 2,884 | 87 | -2,971 | 0 | 0 | 0 | 0 |
| 934 | ENGINEERING & TECH SVCS | 31 | 1 | 1,640 | 1,672 | 35 | -1,707 | 0 |
| 987 | OTHER INTRA-GOVT PURCH | 733 | 22 | 136 | 891 | 19 | -904 | 6 |
| 989 | OTHER SERVICES | 339 | 10 | 10,267 | 10,616 | 223 | -2,769 | 8,070 |
| **0999** | **TOTAL OTHER PURCHASES** | **528,252** | **15,847** | **-25,440** | **518,659** | **10,891** | **33,563** | **563,113** |
| **9999** | **GRAND TOTAL** | **593,553** | **17,334** | **-18,509** | **592,378** | **13,912** | **37,353** | **643,643** |

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

**The total amount of the FY 2023 request reflects $3,232.0 thousand for Overseas Operations Costs