Fiscal Year 2022 President's Budget

Defense Information Systems Agency Cyber

May 2021

Operation and Maintenance, Defense-Wide Summary ($ in thousands)
Budget Activity (BA) 1: Operating Forces/Combat Development Activities

	FY 2020 Actuals	Price Change	Program Change	FY 2021 Enacted	Price Change	Program Change	FY 2022 Request
DISA Cyber	650,340	12,715	-70,707	592,348	11,510	-73,580	530,278

*FY 2020 includes Division A, Title IX and X of the Consolidated Appropriations Act, 2020 (P.L. 116-93), Division F, Title IV and V from the Further Consolidated Appropriations Act, 2020 (P.L. 116-94) and the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116-136).
*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).

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 Strategic Guidance (DSG) and reflects the Department of Defense Chief Information Officer's (DoD CIO) Capability Planning Guidance (CPG). As noted in DISA's Strategic plan, the DISA's mission is to conduct DoD Information Network (IN) operations for the joint warfighter to enable lethality across all warfighting domains in defense of our nation. The DISA plans, engineers, acquires, tests, fields, operates, and assures information-sharing capabilities, command and control solutions, and a global enterprise infrastructure to support the DoD and national-level leadership.

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

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

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 a customized 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 2018 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 Internet protocol 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 Defense Collaboration Service (DCS), global 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

I. Description of Operations Financed: (Cont.)
both external and internal attacks, detecting lateral movement, and fully incorporating a more robust endpoint capabilities in a synchronized and standardized defensive implementation.

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

Cyberspace Activities: Provide engineering, architecture, analytic solutions and technical support for DoD to achieve enterprise situational awareness and resilient DODIN cybersecurity in contested cyberspace.

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

The CAM is the tool which DISA uses to allocate its shared services across the agency's portfolio of programs and component organizations on an evaluated basis and approved by our cost analysis staff. Examples of costs being allocated includes items such as utilities and building operations at the DISA complex, Fort Meade, MD; the Defense Finance and Accounting Services (DFAS) personnel support; and DISANet internal 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 2022: $530,278 thousand)

1. Joint Force Headquarters DoD Information Network (JFHQ-DODIN) (FY 2022: $94,077 thousand): The DISA directs, coordinates, and synchronizes DISA-managed portions of the DoDIN supporting the DoD in 42 countries around the world across the full spectrum of military operations and supports the United States Cyber Command (USCYBERCOM) in its mission to provide secure, interoperable, and reliable operations of the DoDIN. Our primary tasks are to operate and defend the DISA information enterprise, and provide direct support to the USCYBERCOM in the DoDIN Operations (DO) and Defensive Cyber Operations (DCO). This responsibility includes the actions necessary to provide certification, threat identification and intrusion prevention, intrusion detection, and incident response/recovery, of both the Non-secured Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). In order to accomplish this, the NetOps provides the command and control (C2), situational awareness, and defense of the DoD Network across all levels of command, strategic,

I. Description of Operations Financed: (Cont.)
operational, and tactical boundaries. It supports the DoD's full spectrum of war fighting to include support for the intelligence and business missions.

The DISA executes its mission to command and control, plan, direct, coordinate, integrate and synchronize the DoD's Information Network (DoDIN) operations and Defensive Cyber Operations-Internal Defensive Measures (DCO-IDM) globally. Reliable services are delivered worldwide in 42 nations at 3,800 locations. The DISA will manage or execute approximately 200 million managed network assets, in excess of 50,000 telecommunications service orders and circuit actions, 40,000 servers hosting 870 user applications, 17,000 circuits, 55 SATCOM Gateways, 38 Petabytes of storage, 4.5 million DoD identities, 1.6 million to 4.5 million enterprise e-mail Users, 1 million to 4.5 million nobility/voice/video/data over IP users, and blockage and/or tracking of an average of 180 million malicious events per month.

Increasing cyber security threats have expanded our cyber operations mission, both in terms of the breadth (e.g. Enterprise Services) and required depth of defenses in the DO/DCO mission space. Near term, the NetOps will transform its organizational structure consistent with the Joint Information Environment (JIE) and support the USCYBERCOM's mission to detect, diagnose, respond to and prevent cyber threats and attacks. Through the use of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) analysis, the NetOps is evolving the DISA Command Center (DCC) to build out the JIE's Global Enterprise Operations Center (GEOC).

The global NetOps structure also manages the integration of teleport and Satellite Tactical Entry Point (STEP) capabilities into the Department of Defense Information Networks (DoDIN); and provides processes for operational direction, control and maintenance of the DISA enterprise infrastructure and services.

In FY 2015, the Secretary of Defense approved the establishment of the Joint Force Headquarters - DoD Information Networks (JFHQ-DODIN) to address 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 Joint Force Headquarters DoD Information Network (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.

Ultimately, the direct operational support that will be provided by the JFHQ-DODIN to 40+ commands and agencies at Full Operational Capability (FOC) include areas focused on aggregating and sharing intelligence to improve situational awareness and understanding, direct/verify the DoDIN defensive posture and lead the DoDIN incident response, synchronize and de-conflict global and regional DoDIN/DCO-IDM priorities, conduct joint

I. Description of Operations Financed: (Cont.)
planning in support of Contingency Plans (CONPLANs) and Operational/Operations Plan (OPLANs) of all Combatant Commands, and enable mission essential functions of the Components.

2. Information Systems Security Program (ISSP)/Information Assurance (IA)/Public Key Infrastructure (PKI) (FY 2022: $426,406 thousand): The ISSP/IA/PKI mission focuses on delivering DoD-wide enterprise solutions to the COCOMS and the DoD Components ensuring critical mission execution in the face of cyber-attacks. The program provides solutions to harden the network by:

1) 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.

2) Deploying a secure protocol decryption and re-encryption mechanism to protect communications across the Joint Information Environment (JIE) and through the Internet Access Points (IAPs). Efforts include break and inspect of secure socket layer/transport level security (and other) protocols for both outbound and in-bound encrypted traffic.

3) Provides vital situational awareness to senior decision-makers and network defenders that enable attack detection and diagnosis.

4) Supporting safe sharing of information with allies and mission partners, by expanding the cross domain 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).

5) 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.

6) Providing training to the DoD civilians by continuing to generate information assurance and NetOps training used throughout the Department using web enabled tools.

7) Providing public key certificates (PKI) that provide electronic identities for mission critical applications. The PKI supports the infrastructure for the entire DoD enabling information sharing in a secured environment. The PKI satisfies the DoD's Information Assurance (IA) needs for confidentiality, authentication, identification, and verification of data integrity, non-repudiation of communications of transactions, as well as digital signatures.

The JRSS is a joint DoD security architecture comprised of complementary defensive security solutions that remove redundant Information Assurance (IA) protections; leverages enterprise defensive capabilities with standardized security suites; protects the enclaves after 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.

I. Description of Operations Financed: (Cont.)
3. Defense Industrial Base (DIB) (FY 2022: $9,795 thousand): 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 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.

The FY 2022 Direct War and Enduring Costs accounted for in the base budget are as follows:

• Direct War costs accounted for in the Base Budget: $0.0 thousand: Direct War costs are those combat or direct combat support costs that will not continue to be expended once combat operations end at major contingency locations.

• Enduring costs accounted for in the Base Budget: $3,524.0 thousand: Enduring Requirements are enduring in theater and in CONUS costs that will likely remain after combat operations cease.

II. Force Structure Summary:
Not Applicable.

III. Financial Summary ($ in Thousands):

		FY 2021					
			Congressional Action				
A. BA Subactivities	**FY 2020 Actuals**	**Budget Request**	**Amount**	**Percent**	**Appropriated**	**Current Enacted**	**FY 2022 Request**
COVID-19 Supplemental	$10,525	$0	$0	0.00%	$0	$0	$0
Defense Industrial Base (DIB) - Cyberspace Operations	$9,961	$9,788	$0	0.00%	$9,788	$9,788	$9,795
Information Systems Security Program (ISSP) / Information Assurance (IA) - Cyberspace Operations	$540,835	$486,076	$6,686	1.38%	$492,762	$492,762	$426,406
Network Operations (NetOps)/Joint Force Headquarters DoD Information Network (JFHQ-DODIN) - Cyberspace Operations	$89,019	$90,299	$-501	-0.55%	$89,798	$89,798	$94,077
Total	**$650,340**	**$586,163**	**$6,185**	**1.06%**	**$592,348**	**$592,348**	**$530,278**

*FY 2020 includes Division A, Title IX and X of the Consolidated Appropriations Act, 2020 (P.L. 116-93), Division F, Title IV and V from the Further Consolidated Appropriations Act, 2020 (P.L. 116-94) and the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116-136).
*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).

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

B. Reconciliation Summary	Change FY 2021/FY 2021	Change FY 2021/FY 2022
BASELINE FUNDING	**$586,163**	**$592,348**
Congressional Adjustments (Distributed)	10,000	
Congressional Adjustments (Undistributed)	-3,815	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
SUBTOTAL APPROPRIATED AMOUNT	**592,348**	
Fact-of-Life Changes (2021 to 2021 Only)	0	
SUBTOTAL BASELINE FUNDING	**592,348**	
Supplemental	0	
Reprogrammings	0	
Price Changes		11,510
Functional Transfers		0
Program Changes		-73,580
CURRENT ESTIMATE	**592,348**	**530,278**
Less: Wartime Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$592,348**	**$530,278**

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

FY 2021 President's Budget Request (Amended, if applicable)	**$586,163**
1. Congressional Adjustments	$6,185
a) Distributed Adjustments	$10,000
1) Program Increase - Comply to Connect	$10,000
b) Undistributed Adjustments	$-3,815
1) Undistributed Adjustment – Excess to Need – Non-NIP	$-3,815
c) Adjustments to Meet Congressional Intent	$0
d) General Provisions	$0
FY 2021 Appropriated Amount	**$592,348**
2. War-Related and Disaster Supplemental Appropriations	$0
a) OCO Supplemental Funding	$0
3. Fact-of-Life Changes	$0
a) Functional Transfers	$0
b) Technical Adjustments	$0
c) Emergent Requirements	$0
FY 2021 Baseline Funding	**$592,348**

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

4. Reprogrammings (Requiring 1415 Actions)	$0
a) Increases	$0
b) Decreases	$0
Revised FY 2021 Estimate	**$592,348**
5. Less: Item 2, War-Related and Disaster Supplemental Appropriation and Item 4, Reprogrammings	$0
a) Less: OCO Supplemental Funding	$0
FY 2021 Normalized Current Estimate	**$592,348**
6. Price Change	$11,510
7. Functional Transfers	$0
a) Transfers In	$0
b) Transfers Out	$0
8. Program Increases	$57,252
a) Annualization of New FY 2021 Program	$0
b) One-Time FY 2022 Increases	$0
c) Program Growth in FY 2022	$57,252

1) Compensation and Benefits $1,945
Increase in compensation and benefits primarily reflects an internal rephasing. The DISA experienced significant under execution in FTEs, and as a result, the Agency reduced civilian FTE levels in under

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

executing programs and gradually rephased these FTEs across future years. The increase of FTEs represents this year's rephasing level. DISA continues to use a variety of recruiting initiatives such as direct hiring authority, job fairs, cyber excepted service authorities, etc. to return programs to their authorized manpower levels. Additionally, increase are due to compensation and benefits reflects an increase to civilian personnel costs to reflect the revised Federal Retirement System (FERS), civilian pay raise assumption, and performance awards for Non-Senior Executive Service (SES), Senior Level (SL), and Scientific or Professional (ST) employees.
(FY 2021 Baseline: $69,218 thousand; 365 FTEs; +12 FTEs)

2) Information Systems Security Program (ISSP) $55,307
Increase is to support the Services Joint Regional Security Stack (JRSS) execution in accordance with the approved plan at the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM) forum on Aug 27, 2020.

(FY 2021 Baseline: $491,264 thousand)

9. Program Decreases ..... $-130,832

a) Annualization of FY 2021 Program Decreases $0

b) One-Time FY 2021 Increases ..... $-10,000

1) Program Increase - Comply to Connect ..... $-10,000

c) Program Decreases in FY 2022 ..... $-120,832

1) Travel of Persons ..... $-595
Decrease in mission travel is due to major advancements in virtual connectivity as a result of the Covid-19 pandemic.
(FY 2021 Baseline: $1,551 thousand)

2) Information Systems Security Program (ISSP) ..... $-120,165
Decrease is primarily attributable to the integration of the DoD Cyber Situational Awareness Analytic Capabilities (CSAAC) into Joint Regional Security Stack (JRSS) and reduced hardware, software tech refresh requirements for JRSS; a reduction in support for Milcloud NIPRNet sustainment; and a reduction in licensing, training and SME support for the deployment, implementation and maintenance of the Department

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

of Defense (DoD) Chief Information Officer's (CIO's) Comply to Connect (C2C) Framework for DoD.
(FY 2021 Baseline: $491,264 thousand)

3) Direct War and Enduring program changes accounted for in the Base Budget ..... $-72
Direct War costs are those combat or direct combat support costs that will not continue to be expended once combat operations end at major contingency locations. Enduring Requirements are enduring in theater and in CONUS costs that will likely remain after combat operations cease, and have previously been funded in OCO. Detailed justifications for Direct War and Enduring program changes are provided in the Operation and Maintenance, Defense-wide, Volume I Part 2 Book
(FY 2021 Baseline: $3,524 thousand)

FY 2022 Budget Request $530,278

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2020 Actual	2021 Plan	2022 Plan
Information Systems Security Program (ISSP)/Information Assurance (IA)/Public Key Infrastructure (PKI):			
2. CMRS -- How many new user accounts with defined permissions were created in the past 365 days?	2. 820	2. 360 NIPR & 300 SIPR	2. 360 NIPR & 300 SIPR
3. Cyber Situational Awareness Analytic Capabilities (CSAAC) Analytics -- Number of OPT Sensors Deployed/ Maintained. Target: 9000	3.	3.	3.
4. 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 COCOMs.	4. 4 classes	4. 4 classes	4. 4 classes
5. Assured Identity transition to 20,000 devices.	5.	5.	5. 100%
6. Engineering and integration of two Secure Host Baseline (SHB)/WIN10 releases per year. (Target: Number of releases/year)	6. 2	6. 2	6. 2
7. Objective is to protect 100% of internet Facing, DECC hosted, applications with the Web Application Firewall. (Target: Percentage of releases/year)	7.	7. 56%	7. 75%
8. Percentage of Information Assurance Support Environment (IASE) content requests completed within the terms of the Service Level Agreement (SLA). (Target: ticket completion percentage)	8. 97%	8. 95%	8. 95%
9. Integration into the Persistent Cyber Training Environment (PCTE) with the NCR. (Target: number of events)	9. 2	9. N/A	9. N/A
10. Develop and maintain training for 30 role based cybersecurity courses based on DoD Cyber Workforce Framework. (Target: number of courses)	10. 30	10. 30	10. 30
11. Joint Regional Security Stack (JRSS) -- Implement JRSS Management System (JMS) CSAAC analytic capability.			

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2020 Actual	2021 Plan	2022 Plan
	11. 6	11. 6	11. 6
Network Operations (NetOps)/Joint Force Headquarters DoD Information Network (JFHQ-DoDIN) – Cyberspace Operations: 1. JFHQ-DoDIN synchronizes forces to harden the DoDIN. % of task orders completed b. % of planned COCOM CONPLAN and OPLAN defensive cyber support plans completed	 1a. 85% 1b. 85%	 1a. 85% 1b. 85%	 1a. 85% 1b. 85%

V. Personnel Summary:

	FY 2020	FY 2021	FY 2022	Change FY 2020/ FY 2021	Change FY 2021/ FY 2022
Active Military End Strength (E/S) (Total)	**4,895**	**5,061**	**5,083**	**166**	**22**
Officer	989	1,021	1,021	32	0
Enlisted	3,906	4,040	4,062	134	22
Reservists on Full Time Active Duty (E/S) (Total)	**150**	**151**	**151**	**1**	**0**
Officer	87	88	88	1	0
Enlisted	63	63	63	0	0
Civilian End Strength (Total)	**359**	**365**	**377**	**6**	**12**
U.S. Direct Hire	359	365	377	6	12
Total Direct Hire	**359**	**365**	**377**	**6**	**12**
Active Military Average Strength (A/S) (Total)	**4,895**	**5,061**	**5,083**	**166**	**22**
Officer	989	1,021	1,021	32	0
Enlisted	3,906	4,040	4,062	134	22
Reservists on Full Time Active Duty (A/S) (Total)	**150**	**151**	**151**	**1**	**0**
Officer	87	88	88	1	0
Enlisted	63	63	63	0	0
Civilian FTEs (Total)	**359**	**365**	**377**	**6**	**12**
U.S. Direct Hire	359	365	377	6	12
Total Direct Hire	**359**	**365**	**377**	**6**	**12**
Average Annual Civilian Salary ($ in thousands)	**175.6**	**189.6**	**192.9**	**14.1**	**3.3**
Contractor FTEs (Total)	**488**	**488**	**501**	**0**	**13**

V. Personnel Summary: (Cont.)

Personnel Summary Explanations:

*USSOCOM military personnel are reported in the Military Service Estimates. The Military end strength numbers reflect authorized personnel.

*Military end strength net increase of +22 enlisted personnel supports continued force structure growth to provide Cyber support.

*Civilian net increase of +12 FTEs for planned FY 2022 primarily reflects an internal rephasing. The DISA experienced under execution in FTEs. As a result, the Agency reduced civilian FTE levels in under executing programs and gradually rephased these FTEs. The increase of FTEs represents this year's rephasing level. The DISA continues to use a variety of recruiting initiatives such as direct hiring authority, job fairs, cyber excepted service authorities, etc. to return programs to their authorized manpower levels.

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

			Change from FY 2020 to FY 2021			Change from FY 2021 to FY 2022		
		FY 2020 Program	Price Growth	Program Growth	FY 2021 Program	Price Growth	Program Growth	FY 2022 Program
101	EXEC, GEN'L & SPEC SCHEDS	63,013	970	5,235	69,218	1,571	1,945	72,734
106	BENEFIT TO FMR EMPLOYEES	20	0	-20	0	0	0	0
0199	**TOTAL CIVILIAN PERSONNEL COMPENSATION**	**63,033**	**970**	**5,215**	**69,218**	**1,571**	**1,945**	**72,734**
308	TRAVEL OF PERSONS	406	8	1,137	1,551	29	-595	985
0399	**TOTAL TRAVEL**	**406**	**8**	**1,137**	**1,551**	**29**	**-595**	**985**
677	DISA TELECOMM SVCS - REIMBURSABLE	22	0	-22	0	0	0	0
0699	**TOTAL OTHER FUND PURCHASES**	**22**	**0**	**-22**	**0**	**0**	**0**	**0**
771	COMMERCIAL TRANSPORT	40	1	-41	0	0	0	0
0799	**TOTAL TRANSPORTATION**	**40**	**1**	**-41**	**0**	**0**	**0**	**0**
913	PURCHASED UTILITIES (NON-FUND)	43	1	-44	0	0	0	0
914	PURCHASED COMMUNICATIONS (NON-FUND)	119	2	507	628	12	127	767
920	SUPPLIES & MATERIALS (NON-FUND)	252	5	91	348	7	130	485
922	EQUIPMENT MAINTENANCE BY CONTRACT	538,297	10,766	-87,070	461,993	8,778	-70,088	400,683
923	FACILITIES SUST, REST, & MOD BY CONTRACT	10,427	209	-10,636	0	0	0	0
925	EQUIPMENT PURCHASES (NON-FUND)	7,598	152	47,417	55,167	1,048	-14,770	41,445
932	MGT PROF SUPPORT SVCS	7,071	141	-7,212	0	0	0	0
934	ENGINEERING & TECH SVCS	3,209	64	-1,632	1,641	31		1,672
987	OTHER INTRA-GOVT PURCH	122	2	653	777	15	99	891
989	OTHER SERVICES	19,701	394	-19,070	1,025	19	9,572	10,616
0999	**TOTAL OTHER PURCHASES**	**586,839**	**11,736**	**-76,996**	**521,579**	**9,910**	**-74,930**	**456,559**
9999	**GRAND TOTAL**	**650,340**	**12,715**	**-70,707**	**592,348**	**11,510**	**-73,580**	**530,278**

*FY 2020 includes Division A, Title IX and X of the Consolidated Appropriations Act, 2020 (P.L. 116-93), Division F, Title IV and V from the Further Consolidated Appropriations Act, 2020 (P.L. 116-94) and the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116-136).
*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).

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

The FY 2020 Actual does not match the data in the O-1 exhibit; the FY 2020 Actual reflects the correct amount.