Fiscal Year (FY) 2019 President's Budget

Operation and Maintenance, Defense-Wide

Defense Information Systems Agency

February 2018

(This page intentionally left blank)

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2019 President's Budget

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

	FY 2017 Actuals	Price Change	Program Change	FY 2018 Estimate	Price Change	Program Change	FY 2019 Estimate
DISA	1,508,429	25,968	475,305	2,009,702	30,645	66,583	2,106,930

* The FY 2017 Actual column includes $48,814.0 thousand of FY 2017 Overseas Contingency Operations (OCO) Appropriations Funding (PL 115-31).
* The FY 2018 Estimate column excludes $64,137.0 thousand of FY 2018 OCO Appropriations Funding.
* The FY 2019 Estimate column excludes $111,702.0 thousand of FY 2019 OCO Appropriations funding.

I. Description of Operations Financed:

The Defense Information Systems Agency (DISA), a combat support agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. DISA implements the Secretary of Defense's Defense Strategic Guidance (DSG) and reflects the DoD CIO's Capability Planning Guidance (CPG). The DoD CIO vision is "to reduce sustainment costs and improve warfighting capability over time."

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. In short, the DISA provides global net-centric solutions in the form of 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 the only combat support agency charged with connecting the force by linking processes, systems, and infrastructure to people. This budget anticipates impacts to our operations from the DoD's 26-point IT transformation plan known as the IT

I. Description of Operations Financed (cont.)

Enterprise Strategy Roadmap (ITESR). The Deputy Secretary of Defense signed the ITESR and the CIO CPG in March 2015.

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

- **Evolve the Joint Information Environment (JIE) -** Evolve a consolidated, collaborative, and secure JIE, enabling end-to-end information sharing and interdependent enterprise services across the Department that are seamless, interoperable, efficient, and responsive to joint and coalition warfighter requirements;
- **Provide Joint Command and Control (JC2) and Leadership Support -** Engineer, provide, and enhance C2 and mission partner information sharing capabilities to enable decision makers with the ability to exercise authority and direction over assigned and attached forces and resources while rapidly and effectively sharing information across the strategic, operational, and tactical spectrum of operations. DISA will lead the development and evolution of JC2 capabilities used to plan and execute the full range of joint, interagency, and multinational military operations;
- **Operate and Assure the Enterprise as a part of the Department of Defense Information Network (DODIN) -** Command and control, plan, direct, coordinate, integrate and synchronize the DODIN Operations (DO) and select Defensive Cyber Operations (DCO) to secure, operate, defend and protect the DODIN across the full spectrum of military operations. Through our partnership with United States Cyber Command (USCYBERCOM), evolve our cyber and network capabilities to function under dynamic conditions responding to increasing warfighter information requirements, increased demand for operational efficiencies, and shifts in the global defense posture. Organize to consistently and rapidly adapt to changing circumstances around the world - on

I. Description of Operations Financed (cont.)

demand, using advanced technologies and standardized tool sets, synchronized processes and procedures, and, a highly trained cyber workforce and

- **Optimize Department Investments** – Enable the Department to maximize use of its resources by providing cost efficient capabilities; an effective and defensible infrastructure; and standardized support services, business processes, and policies that enable the rapid infusion of technology into the enterprise.

These four Strategic Goals focus DISA's efforts on a target objective state that embodies "a secure connection to a computing environment provided by both commercial and government computing centers and big data storage, interconnected with a mesh of fixed and wireless transport, protected by a single security architecture, whose information resources held in the cloud are reachable by various mobile devices, and accessible by credentialed users eliminating anonymity from the network."

Today, DISA is a combined military, federal civilian, and support contractor workforce of 16,483 people touching 100 countries. DISA believes the key to a global, information-based DoD Enterprise is not to design the solution, but design the framework for constructing the solution. DISA does not know what the next engagement will look like, and the DISA cannot build, nor does the DISA want to build, specific systems to try to solve every possible problem. Rather, DISA is creating a global enterprise infrastructure based on common standards so that innovative, flexible, and efficient solutions can be rapidly deployed to the warfighter--in commercial parlance, DISA provides cloud computing services to DoD.

To realize this goal, the Department must revolutionize its ability to react, share, collaborate, and execute. The Department needs a common platform of capabilities and

I. Description of Operations Financed (cont.)

services that enable new applications and solutions to be built, and empower their rapid development and fielding. This common platform will allow users in any location, service or DoD agency, and using any computing platform to access and process information. These are the architectural concepts that have revolutionized the commercial IT industry over the past decade.

This global enterprise infrastructure begins with an increasingly robust, capable computing platform. DISA meets this need with our Defense Enterprise Computing Centers (DECCs), which provide storage, computing power, application hosting, and content delivery worldwide. Collectively these facilities provide a robust enterprise computing environment consisting of over 12,000 servers, over 50,000 terabytes of storage, approximately 368,000 square feet of raised floor, redundant connectivity to the DISN core, 22 mainframes, and support to over four million users. Upon this foundation of information transport and robust computing, DISA is building a framework of common enterprise services, designed to be transparent to the user and available to all. These services include network authentication and identity management, online collaboration, search, messaging, and security.

To be effective in the current world environment there must also be comprehensive and integrated cyber protection for this infrastructure. DISA is in the midst of an effort to improve the security and defense capabilities of our military networks using improved sensoring for intrusion detection and reporting, demilitarized zones (DMZ), filtering, and proxying to protect our core network services from internet threats.

The DISA has reprioritized resources within its programs to support the Department's Global re-balancing initiative. Examples include reprioritizing DISN Tech Refresh

I. Description of Operations Financed (cont.)

funding to support investments being made in concert with consolidation of networks in Europe (reflecting the downsizing of the Defense footprint), and reprioritizing Multi-National Information Systems (MNIS) investments to address PACOM near-term requirements for expanded Coalition connectivity in their area of responsibility.

The DISA aligns its program resource structure across six mission areas. The first five mission areas reflect customer support strategies. The sixth mission area represents the DISA's critical special missions support to the Commander in Chief. These mission areas reflect the DoD goals and represent the DISA's focus on executing its lines of operation:

- **Transition to Net Centric Environment**: Transition to a net-centric environment to transform the way DoD shares information by making data continuously available in a trusted environment.
- **Eliminate Bandwidth Constraints:** 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:** Operate, protect, defend, and sustain the enterprise infrastructure and information sharing services; and enable Command and Control.
- **Exploit the DODIN for Improved Decision Making:** Transition to 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:** Deliver capabilities, based on established requirements, more effectively, economically, and efficiently than the DISA does today.

I. Description of Operations Financed (cont.)

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

DISA continues to use the Cost Allocation Model (CAM) to assign costs of shared services to products and services. The Cost Allocation Model identifies the total cost of a program and avoids unintended subsidy to the Defense Working Capital Fund, gains visibility and insight into 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 a basis evaluated and approved by our cost analysis staff. Examples of costs being allocated include items such as utilities and building operations at the DISA complex at Ft. Meade, MD; Defense Finance and Accounting Services (DFAS) personnel support; and DISANet internal IT costs. The CAM tool organizes DISA programs and component organizations into categories to which specific costs are applicable. For example, activities outside of the Fort Meade complex -- such as Joint Interoperability Test Command (JITC)-- are not charged a share of the utilities and building operations at the DISA complex at Ft. Meade, MD, though they are charged a share of the DFAS personnel support and DISANet internal IT costs. The STRATCOM Field Office, which is not at Fort Meade and gets its IT support from U.S. Strategic Command (STRATCOM), 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 Defense Working Capital Fund activities.

I. Description of Operations Financed (cont.)

Mission Area: Transition to Net Centric Environment (FY 2019: $233,443 thousand)

1. Net-Centric Enterprise Services (NCES)(FY 2019: $61,220 thousand): The Operations Center provides a portfolio of critical enterprise services to warfighter, business, and intelligence end-users on the Secret Internet Protocol (IP) Data network and the Sensitive but Unclassified (SBU) IP Data network. This portfolio of services allows more than two million authorized DoD users to collaborate across COCOMs/Services/Joint Staff/Agencies using a suite of web-accessible collaboration capabilities supporting DoD and other supporting users. The portfolio provides a resilient and flexible infrastructure that enables a secure collaborative environment that facilitates information sharing in the DoD from any location at any time; and a robust Enterprise Messaging service that decouples the producer from the consumer, allowing consumers to easily subscribe to information that supports their evolving missions and for producers to rapidly and efficiently publish both perishable and non-perishable data without the need to specify the recipients.

This portfolio includes evolving enterprise services such as: the DoD Visitor capability that enables the enterprise user vision of "go anywhere in the DoD, login, and be productive"; and support to an Identity Synchronization Service to support its use to populate Active Directories Department-wide as well as supporting dual authentication to enterprise services using the user's credentials. The portfolio integrates the enterprise services with DoD Enterprise Email that consolidates DoD corporate e-mail, centralizes all e-mail management department-wide, provides the user with a single email address that will be used throughout their career, and is accessible from any location at any time; and the DoD Enterprise Portal Service that provides users with a flexible web-

I. Description of Operations Financed (cont.)

based hosting solution to create and manage mission, community, organization, and user focused sites.

The individual capabilities within the portfolio of services provide the user with the flexibility to couple the services in varying ways and provide access to web and application content, warfighter information, and forward-cached critical data in a secure environment.

In addition, this portfolio supports application rationalization efforts within DISA. Specifically, the Agency will identify and prioritize legacy DISA and Joint Service Provider (JSP) applications for modernization to facilitate the transition of those applications to cloud hosting environments (both commercial and DoD on premise solutions).

2. Department of Defense Information Network Engineering Services (DODIN ES)(FY 2019: $51,316 thousand): Enterprise Engineering supports DODIN End-to-End (E2E) Systems Engineering, Interface Standards, and a Modeling and Simulation (M&S) environment which enables the development of DISA and DoD IT technical architectures and capabilities that are interoperable and performance-oriented. Effective E2E system engineering is applied by implementing model based systems engineering (MBSE) to capture and resolve technical problems across the DODIN. E2E systems engineering develops and maintains DODIN Convergence Master Plan (GCMP) and Unified Communication and Collaboration (UC&C) architecture to integrate DODIN capabilities. These capabilities ensure that both the DoD and DISA's infrastructure services and applications are planned, implemented, and assessed/improved to meet performance objectives cost-efficiently.

I. Description of Operations Financed (cont.)

As the Agency's senior authority on scientific, technical and engineering matters, the Office of the Chief Technology Officer (OCTO) promotes centralized, coordinated technology policy, direction, standards, and leadership for DISA/DoD. OCTO conducts extensive technology outreach (including weekly technical exchange meetings (TEM) with DoD CIO, federal agencies, industry, and academia to identify best practices, methodologies, material solutions, mature capabilities, and enterprise services. OCTO ensures environmental support and maintenance is provided during transition of technology solutions. OCTO leverages existing relevant technology and capabilities resident throughout the DoD to achieve a flexible and rapidly reconfigurable environment for analysis of emerging technologies. OCTO performs security engineering and accreditation of products while undergoing assessment within the Technology Analysis Center (TAC).

3. Background Investigation IT Systems (FY 2019: $117,642 thousand): The Interagency Deputies Committee and the Office of Management and Budget (OMB) has determined that the responsibility for the development and sustainment of a new Federal Government background investigation information technology (IT) system(s) will transfer from the Office of Personnel Management (OPM) to the Department of Defense. The DISA will be responsible for the development, implementation, and sustainment of this new background investigation system. The acquisition and implementation planning strategy will support the Federal workgroups requirements gathering and provide Government-wide tools to assist agencies with workforce management that comply with new Federal Investigative Standards. The aim is to avert or eliminate the continuous and dynamic threat of identity theft, financial espionage and other attacks on personal information, while providing a secure basis for background investigations necessary to Federal Government operations.

4. Other Programs (FY 2019: $3,265 thousand): The funding associated with other programs is primarily for the sustainment of systems and hardware costs for DISA.

I. Description of Operations Financed (cont.)

Mission Area: Eliminate Bandwidth Constraints (FY 2019: $217,754 thousand)

1. Standardized Tactical Entry Point (STEP) (FY 2019: $1,230 thousand): The Standardized Tactical Entry Point (STEP) program is a suite of DoD Satellite Communications (SATCOM) Gateways that links deployed tactical users to the Defense Information System Network (DISN). Through the Defense Satellite Communications System (DSCS), STEP provides multi-media telecommunications services at extremely high throughput for deployed forces during operations and exercises.

This program is vital to ensure the tactical users' access to DISN services. The STEP program provides centralized integration capabilities, contingency capacity, and the necessary interfaces to meet Combatant Commands, Services, and Agency requirements to support world-wide operations.

2. DoD Teleport Program (FY 2019: $23,441 thousand): The Department of Defense (DoD) Teleport system is a collaborative investment that upgrades telecommunications capabilities at selected Standardized Tactical Entry Point (STEP) sites. The Teleport system provides deployed forces with improved interfaces for multi-band and multimedia connectivity from deployed locations anywhere in the world to online Defense Information Systems Network (DISN) Service Delivery Nodes (SDN) and legacy tactical command, control, communications, computers, and intelligence (C4I) systems. The Teleport system facilitates interoperability between multiple Satellite Communications (SATCOM) systems and deployed tactical networks, thus providing the user a seamless interface into the DISN and legacy C4I systems. Teleport integrates multi-band, multi-mode satellite capabilities to provide connectivity for deployed tactical communications systems.

I. Description of Operations Financed (cont.)

Teleport has been deployed incrementally as a multi-generational program, and a Full Deployment (FD) was authorized by ASD/NII on February 18, 2011. The DoD Teleport upgrade fills several capability gaps by adding communications support in the Ultra High Frequency (UHF), Extremely High Frequency (EHF), military and Commercial SATCOM frequency bands, which represents a ten-fold increase to the throughput and functional capabilities of these STEP sites. Teleport Generation 3 will field three satellite gateway enhancements in three phases, and the full installation and integration of these enhancements will provide increased satellite connectivity and an expansion of capacity and throughout, which will effectively strengthen DoD's communications and support to tactical and deployed warfighters worldwide. The primary beneficiaries of the Teleport investment are the DoD Combatant Commanders, Military Departments, Defense Agencies and the warfighter.

3. Defense Spectrum Organization (DSO) (formerly called Joint Spectrum Center) (FY 2019: $36,178 thousand): The DSO is leading efforts to transform electromagnetic spectrum (EMS) management to support future operations and warfare. The EMS plays a critical role in national security and is fundamental to all US and coalition military operations. The DSO is comprised of a Strategic Planning Office (SPO), the Joint Spectrum Center (JSC), the Global Electromagnetic Spectrum Information System (GEMSIS) Program Management Office (PMO), and the Business Management Office. The DSO SPO provides spectrum-planning strategies; advocates and defends DoD's EMS needs in national and international forums; and addresses spectrum-related technology issues in policy development and execution. The DSO JSC provides deployable spectrum management support to Combatant Commands (COCOMS), coalition headquarters, and Joint Task Forces (JTFs). The JSC Joint Spectrum Interference Resolution (JSIR) Program provides assistance to operational units to include deployed support to forward-based forces. The JSC mission is integral to vital

I. Description of Operations Financed (cont.)

activities such as information operations, electronic warfare, and other Joint Staff directed projects.

4. Defense Information Systems Network (DISN) Enterprise Activities (EA) (FY 2019: $134,159 thousand): Circuit sustainment, Satellite Communication and National and Presidential Communication requirements enable the DISN to deliver an integrated platform to transport bandwidth and information services on DoD's legacy and Internet Protocol (IP) networks and provide command and control capabilities in support of emerging joint operations. Circuit funding provides circuit management activities to include transition to new contracts, DISN Core optimization, surveys, provisioning, and associated engineering. Satellite Communication funding provides for: SATCOM systems engineering; the migration of Global Broadcast System (GBS) bandwidth management functions to the enterprise infrastructure by the GBS Joint Program Office; the operation, engineering, sustainment, and technical support for the Defense Satellite Communications system (DSCS) including contract support services for DSCS equipment. Special Communication Requirements fund the lifecycle support for the Enhanced Pentagon Capability/Survivable Emergency Conferencing Network (EPC/SECN) switch system that supports the survivable Nuclear Command and Control voice system for the National Command Authority.

Beginning in FY 2017, the DISN portfolio includes four core DISN capabilities that were previously funded through the DISN Subscription Services (DSS) under the DISA DWCF. These four DISN capabilities, whose support is critical to the National Security and DoD-wide enterprise missions, are transferring to the DISN appropriated missions, and are deemed core DISN capabilities whose funding mechanism should be from direct appropriations rather than from the customer orders and reimbursements. They include the following:

I. Description of Operations Financed (cont.)

- **Interoperability and Internet Protocol (IP) Enabling.** The DISN Interoperability is responsible for integration of voice, video, and/or data services delivered ubiquitously across an interoperable, secure, and highly available IP network infrastructure. The IP enabling provides management and registration of all IP number resources for the DoD and is recognized as the DoD agent for IP number management with external Internet Governance organizations. It is also responsible for planning, managing, and sustaining delivery of Domain Name System (DNS) capabilities for the global Internet and for the classified and unclassified Internet Protocols (IP). In addition, it provides the WHOIS capability for database queries relating to IP number registrations and .MIL domain information for the benefit of the DoD and Intelligence Community organizations.

- **Defense Red Switch Network (DRSN).** The DRSN is a global, secure voice service providing the President, the Secretary of Defense, the Joint Chiefs of Staff, the Combatant Commands and selected agencies with Nuclear Command, Control, and Communications (NC3) secure voice and voice conferencing capabilities up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level. The DRSN consists of military departmental and Agency-owned secure voice switches connected by a DISA provided transport backbone.

- **Joint Worldwide Intelligence Communications System (JWICS).** JWICS is a (TS/SCI) high-speed multimedia communication service between SCI users designed to support the Intelligence Community through the Defense Intelligence Agency (DIA) Regional Support Centers (RSCs) and operates on the DISN. It provides real-time voice, video, and data communications and collaboration capabilities in support of DoD, the National Intelligence Community, and the National Command Authority (NCA).

I. Description of Operations Financed (cont.)

Finally, in FY 2017, the circuit transition and management activities are being eliminated under the DISN appropriated missions in favor of a direct customer reimbursement approach. They provided planning, surveys, engineering, and physical circuit implementation support, as well as capacity management contract transition, that are critical to the sustainment of DISN.

5. Defense Information Systems Network (DISN) Infrastructure Services (formerly called DISN Subscription) (FY 2019: $22,746 thousand): The DISN provides secure voice, video, and data services over a global fiber optic network that is supplemented by circuitry obtained from the commercial sector. DISN subscription services are described as follows: Data Services provide SIPRNet as well as NIPRNet capabilities. Voice Services provide day-to-day commercially competitive services plus unique secure military requirements. Voice Services includes the operation of unclassified and classified Voice over IP services. Centralized Services includes provisioning support to DISN users and operators and network management support to all programs that make up the DISN as described above.

Mission Area: DODIN Network Operations and Defense (FY 2019: $518,781 thousand)

1. Network Operations (NetOps) (FY 2019: $92,815 thousand): 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 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 USCYBERCOM in DODIN Operations (DO) and Defensive Cyber Operations (DCO). This responsibility includes the actions necessary

I. Description of Operations Financed (cont.)

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, NetOps provides the command and control (C2), situational awareness, and defense of the DoD Network across all levels of command: strategic, operational and tactical boundaries. It supports DoD's full spectrum of war fighting to include support for intelligence and business missions.

DISA executes its mission to command and control, plan, direct, coordinate, integrate and synchronize 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. 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, 4.5M DoD identities, 1.6M to 4.5M Enterprise Email Users, 1M to 4.5M Mobility/Voice/Video/Data over IP users, and blockage and/or tracking of an average of 180M 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, NetOps will transform its organizational structure consistent with the Joint Information Environment (JIE) and support 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, NetOps is evolving the DISA Command Center (DCC) to build out the JIE's Global Enterprise Operations Center (GEOC).

I. Description of Operations Financed (cont.)

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. JFHQ-DODIN's mission is to exercise command and control of DODIN Operations and Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) globally in order to synchronize the protection of 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 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 USCYBERCOM and subordinate headquarters and 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 DoD's IT infrastructure and applications against a growing international cyber threat and an increasing level of insider threats.

I. Description of Operations Financed (cont.)

Ultimately, the direct operational support that will be provided by JFHQ-DODIN to 40+ commands and agencies at FOC include areas focused on aggregating and sharing intelligence to improve situational awareness and understanding, direct/verify the DODIN defensive posture and lead DODIN incident response, synchronize and de-conflict global and regional DODIN/DCO-IDM priorities, conduct joint planning in support of CONPLANs and 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 2019: $289,877 thousand): The ISSP/IA/PKI mission focuses on delivering DoD-wide enterprise solutions to COCOMS and 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 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 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.

I. Description of Operations Financed (cont.)

- 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 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);

- 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;

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

- 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 Joint Regional Security Stacks (JRSS) are 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

I. Description of Operations Financed (cont.)

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 DoD's Joint Information Environment.

In FY 2019, DISA will consolidate the Comprehensive National Cybersecurity Initiative (CNCI) with ISSP/IA/PKI. This consolidation will streamline and simplify the budgeting, execution and reporting of resources for similar capabilities. This consolidation also allows for better management of the Cybersecurity Portfolio by its major components aligning to the Department's Cyber Strategic Goals and Objectives:

- Endpoint
- Perimeter
- Situational Awareness
- Joint Enablers
- Workforce Development

3. Comprehensive National Cybersecurity Initiative (CNCI) (FY 2019: $0 thousand): The Cybersecurity Program focuses its efforts on a net-centric approach that addresses the Department of Defense (DoD) security demands on a DoD-wide scale. In FY 2019 CNCI is consolidated with ISSP/IA/PKI for better management of the Cybersecurity Portfolio.

4. Field Commands and Field Offices (FY 2019: $100,919 thousand): In DISA's role as a Combat Support Agency, DISA's Field Commands and Field Offices support our Mission Partners (i.e., Combatant Commands, Services, Agencies). They provide specialized support for the National Military Command Center (NMCC). Regional DISA NetOps Centers (DNCs) with physical presence led by military O6s (Field Command/Field Office) support each Geographic and Functional Combatant Command (CCMD). Our support to the CCMDs

I. Description of Operations Financed (cont.)

includes preparing and publishing DISA Support Plans for all CCMD Theater Campaign Plans, Global Campaign Plans and contingency plans, as well as reviewing more than 50 Operational Plans (OPLANS) annually. Field Commands and Field Offices actively participate in Joint and coalition exercises. Field Commands and Field Offices conduct assessments of the threat and hazards, vulnerability, and risk to DoD owned Defense Critical Infrastructure (DCI) and the inter- and intra-dependencies needed to accomplish required DoD missions in accordance with Department of Defense Directive (DoDD) 3020.40, DoD Policy and Responsibilities for Critical Infrastructure.

DISA's five Field Command DISA NetOps Centers (DNCs) operate and assure the DISA enterprise infrastructure while laying the groundwork for introduction of new DISA capabilities and upgrades. The Field Commands and six Field Offices serve as DISA's forward direct support element to the CCMDs, provide customer service support and requirements advocacy for all mission partners in their theater of responsibility who subscribe, or plan to subscribe, to DISA's existing or emerging information products and services. These relationships enable effective coordination and information exchange in support of the Services, new capabilities, policy, and planning. In a partnership and collaborative effort, DISA works with the Joint Staff (JS) and CCMDs in developing the solutions to specific warfighting capability gap requirements identified in their Integrated Priority Lists to the Chairman of the Joint of Staff.

DISA and its Field Commands are directly involved in the evolution to the JIE. For example, the DNC Europe has stood up as the Enterprise Operations Center (EOC) for the European and African Theaters consistent with JIE. DNC PACOM and DNC CENTCOM will also transition into Regional EOCs for their respective geographical areas with JIE, taking on expanded responsibilities to direct operations and defend the DODIN by assuring system and network availability, information delivery, and information protection across

I. Description of Operations Financed (cont.)

strategic, operational, and tactical boundaries in support of DoD, CCMDs, Services, Agencies and the Joint Staff. Continuity of Operations (COOP) plans and exercises assure that the capability exists to continue essential functions and operations across a wide range of potential emergencies. The DISA and DODIN Sector Critical Infrastructure Program (CIP) identifies, characterizes and prioritizes the DODIN Sector and DISA assets, which includes assessing critical C4I components and capabilities to support the execution of CCMDs missions.

Additional missions include: 1) the NATO (Brussels) Field Office ensures U.S. interests are considered in all NATO planning and design efforts to facilitate U.S. and NATO C4ISR interoperability; and, 2) the Ministry of Communications and Information Technology (MCIT) for transforming the Information and Communication Technology (ICT) in support of the business stabilization mission while encouraging strategic economic growth within Afghanistan.

5. Joint Staff Support Center (JSSC) (FY 2019: $25,641 thousand): JSSC provides 24x7 Command and Control (C2) operational support to the President, Secretary of Defense, Joint Staff (JS), Combatant Commanders, and other National-level leaders through global monitoring, maintenance and support of Joint C2 systems, direct operational support to the Deputy Director for Operations J3, comprehensive information assurance and continuous oversight. JSSC also operates and maintains critical decision support system for the National Military Command Center (NMCC) and the National Joint Operations-Intelligence Center in the Pentagon and at Site R.

JSSC also provides 24x7 watch/monitoring of nuclear support operations for C2, Communications, Computer and Intelligence systems for worldwide situational monitoring,

I. Description of Operations Financed (cont.)

rapid decision-making and force direction. Operation services provide strategic threat operational warning, situational awareness, course of action development, and national senior leadership decision-making through sustainment of systems such as Global Command and Control System – Joint, Processing and Display System-Migration, and Nuclear Planning and Execution System. Sustainment of these capabilities is assured through a robust Continuity of Operations capability at an alternate installation (Site R). JSSC also provides full-service television production and multimedia support (studio and remote video and audio recordings, electronic graphics, post production editing for training, informational, gun camera and battle damage assessment assistance, guidance for video teleconferencing networks and operations, and operation of the NMCC secure cable television system) to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the Joint Staff and other DoD agencies. In addition, JSSC provides tactical, strategic, and collaborative planning support for various JS IT initiatives such as NMCS transformation and JS IT migration. JSSC also provides valuable assistance and DISA liaison and customer advocacy support to the Joint Staff Hampton Roads and other regional mission partners as they transition their IT services to DISA-based offerings, resulting in horizontal fusion across all projects being worked by DISA. Operations and Maintenance (O&M) resources include civilian pay and benefits, travel and training as well as sustainment support required to keep fielded systems fully operational during its life cycle, including maintenance of operational environments.

6. Defense Industrial Base (DIB) (FY 2019: $9,529 thousand): The DISA, in concert with the Defense Industrial Base Cyber Security Task Force (DIBCS), is a critical enabler in securing DoD data on 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 USCYBERCOM operations, intelligence, and analysis devoted exclusively to cyber indications and warning,

I. Description of Operations Financed (cont.)

intrusion detection, incident analysis, incident response, information sharing/knowledge management, and planning. Additionally, this initiative provides critical system enhancements and new CYBERCOM 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.

Mission Area: Exploit the DODIN for Improved Decision Making (FY 2019: $810,809 thousand)

1. Global Command and Control System-Joint (GCCS-J) (FY 2019: $104,531 thousand): The GCCS-J is DoD's Joint Command and Control (C2) System of record providing the foundation for migration of service-unique C2 systems into a joint, interoperable environment. The GCCS-J incorporates the core planning and assessment tools required by Combatant Commanders and their subordinates and the Joint Task Force (JTF) Commanders while meeting the readiness support requirements of the Services. Adaptive Planning and Execution Joint Planning Services are being developed to modernize the adaptive planning functions in a net-centric environment. The DISA, through its Joint C2 entities, continues to provide critical C2 capabilities to the Commander-in-Chief, Secretary of Defense, National Military Command Center, COCOMs, Joint Force Commanders, and Service Component Commanders. The DISA portfolio includes funding in support of GCCS-J to include the Joint Operations Planning and Execution Services (JOPES) which supports an expanding Adaptive Planning capability mission.

2. Global Combat Support System-Joint (GCSS-J) (FY 2019: $16,802 thousand): GCSS provides a Joint Logistics Common Operational Picture (JLogCop) and Decision Support Tools to ensure the right personnel, equipment, supplies, and support are in the right

I. Description of Operations Financed (cont.)

place, at the right time, and in the right quantities across the full spectrum of military operations. The GCSS Program continues to develop new and enhanced capabilities to meet critical requirements of the joint logistics warfighter on-time and within budget. GCSS provides actionable information in the form of WatchBoards and widgets in the form of reports and mapping visualizations. A widget is a generic term for a small, stand-alone, downloadable application which looks and acts like traditional apps, but are implemented using web technologies. The benefit for the end user is that the widget provides access to multiple capabilities from one workspace. GCSS supports the mission of the joint logisticians who are the planners, executors, and controllers of the core logistic capabilities.

3. National Military Command System (NMCS) (FY 2019: $7,008 thousand): National Military Command System (NMCS) provides the President, Office of the Secretary of Defense (OSD), Chairman of the Joint Chiefs of Staff, National Military Command Center (NMCC) and NMCC Site R, and the Executive Travel Fleet with the ability to execute C2 over all US military forces across the full spectrum of threats/contingencies. Within the Strategic and National Command, Control, Communications, and Intelligence (SNC3I) Joint Systems Engineering and Integration Office (JSEIO), DISA performs engineering support to meet its assigned NMCS Systems Engineer responsibilities, per Department of Defense Directive (DoDD) S-5100.44 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3280.01B, to provide the Joint Staff with operationally efficient and cost-effective engineering solutions to ensure that NMCS components and facilities satisfy operational requirements including emergency messaging, situational awareness, crisis action, and information management. NMCS engineering projects support DISA's mission of providing responsive, timely, and accurate information to the warfighter.

I. Description of Operations Financed (cont.)

4. Senior Leadership Enterprise (SLE)/Logistics Support Activities (LSA) (FY 2019: $148,525 thousand): This program supports National Leadership Command Capabilities and is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.

5. Combined Advanced Applications (FY 2019: $38,836 thousand): This program supports National Leadership Command Capabilities and is classified. Details provided for this program are submitted in appropriately classified DoD exhibits.

6. Multinational Information Sharing (MNIS) Program (FY 2019: $0 thousand): The MNIS Program is a portfolio of four coalition information sharing capabilities: Combined Enterprise Regional Information Exchange System (CENTRIXS) (to include the CENTRIXS Cross Enclave requirement), Pegasus (formerly Griffin), Unclassified Information Sharing (UISS) and Combined Federated Battle Laboratory Network (CFBLNet). Through this portfolio, MNIS provides information sharing capabilities designed to enable and improve sharing of operational and intelligence information among US forces and multinational partners.

The CENTRIXS supports intelligence and classified operations and information exchange and/or sharing at the Secret Releasable (REL) level. There are multiple, cryptographically-isolated enclaves serving various communities of interest (COI) that support multinational efforts in Iraq and Afghanistan, as well as the Overseas Contingency Operations (OCO) and counter-narcotics operations. The CENTRIXS is regionally focused and Combatant Command (COCOM) centric.

An improvement to the CENTRIXS coalition network, Common Mission Network Transport (CMNT), provides distinct and permanent transport capabilities; enabling network

I. Description of Operations Financed (cont.)

operation centers to priority command and control information more efficiently. CMNT supports DoD instruction 8110.1 guidance for integrating CENTRIXS and other operational networks into existing DoD general service communications infrastructure as a separate network servicing all DoD MNIS requirements. This capability provides a common transport for encrypted traffic. CMNT will be the established encrypted network to facilitate the movement of virtual private network traffic between segments.

Pegasus interconnects the National Command and Control (C2) systems of Combined Communications Electronics Board (CCEB) Nations using Cross Domain Solutions (CDS) that enable information sharing to facilitate situational awareness and operational planning/execution. Pegasus has a strategic focus and is member nation centric.

CFBLNet is a laboratory environment which utilizes a distributed Wide Area Network (WAN) as the vehicle to experiment with new capabilities by conducting Research and Development, Trials and Assessment (RDT&A) initiatives. The CFBLNet is managed by DISA and consists of distributed and integrated network architecture of Combined, Joint, and Military Service infrastructure components (networks, database servers, application servers, client workstations, etc.). Unclassified Information Sharing Services (UISS) capability is an enterprise solution designed to meet unclassified collaboration and information sharing requirements of joint and coalition military organizations. UISS provides the United States COCOMs a unique operational capability necessary to support coordination, cooperation, and collaboration with mission partners. The overarching objective of the UISS is to provide a collaborative internet portal to share unclassified information to the COCOMs. The UISS capability will be a web-based, "non-mil", information sharing and collaboration tool that may be accessed anytime, from anywhere, by any user with an Internet connection including web-enabled mobile personal devices. HARMONIEWeb (HWeb) supports unclassified communications and collaboration connections

I. Description of Operations Financed (cont.)

that bridge the gap between government, non-government, coalition, interagency, and international organizations.

In FY 2019, the Multinational Information Sharing (MNIS) Program responsibilities and resources are functionally transferred from DISA to USAF to develop and field a Mission Partner Environment to address COCOM data sharing requirements with allies.

7. Joint Service Provider (JSP) (FY 2019: $477,916 thousand): The Joint Service Provider (JSP) provides Information Technology infrastructure and office automation systems, components, supporting software, and IT support services for the Office of the Secretary of Defense (OSD), Washington Headquarters Services (WHS), Pentagon Force Protection Agency (PFPA), Consolidated Adjudication Facility (CAF), and other WHS-supported users and communities supported within the Pentagon Reservation and other areas in the National Capitol Region. The funding levels represent transfers from the legacy organizations, WHS-EITSD, Joint Staff, and OAA-Army, to support their ongoing consolidated mission. The purpose of the JSP IT Program is to provide end-user computing capabilities needed to fulfill the JSP components' missions, and is comprised of departmental local area networks, computer servers, network storage subsystems, network printers, workstations, a full suite of desktop office applications, development of custom tools and application, and system firmware integrated into a distributed computing network environment for unclassified and classified information processing. The program provides JSP organizations with ubiquitous access to reliable, decision-quality information through a net-based services infrastructure. Funded initiatives include support of the Deputy Secretary of Defense Pentagon IT consolidation memorandum which promotes the consolidation of common IT systems and, where proper analysis suggests, additional consolidation of IT support organizations and structures will be accomplished. Commonality will be leveraged wherever it makes sense, consistent with agency business

I. Description of Operations Financed (cont.)

processes, to better support mission requirements in local and national emergencies.

8. Other Programs (FY 2019: $17,191 thousand): The funding associated with other programs is primarily for the infrastructure costs for DISA's interoperability facility in the National Capital Region.

Mission Area: Deliver Capabilities Effectively/Efficiently (FY 2019: $87,590 thousand)

1. Management Headquarters (FY 2019: $36,749 thousand): Management Headquarters funding is utilized for salaries and operating expenses associated with the Command and Executive Staff and their key control organizations, which provide oversight, direction, and control of DISA activities. Command and Executive staffs enable DISA to continuously operate and assure a global net-centric enterprise in direct support to the joint warfighter, national level leaders, and other mission and coalition partners across the full spectrum of operations.

2. Pentagon Reservation Maintenance Revolving Fund (PRMRF) (FY 2019: $20,564 thousand): United States Code, Title 10, Section 2674 established the Pentagon Reservation Maintenance Revolving Fund (PRMRF), authorizing the Secretary of Defense to establish rates and collect charges for space, services, protection, maintenance, construction, repairs, and alterations of facilities provided at the Pentagon Reservation.

3. Shared Services Units/Program Executive Offices (FY 2019: $30,277 thousand): This activity funds foundational operating capabilities for DISA, such as: financial management, information technology, strategic planning, manpower/personnel security, and acquisition products and services to all agency programs and business areas world-wide.

I. Description of Operations Financed (cont.)

4. Other Programs (FY 2019: $0 thousand): The Foreign Military Sales (FMS) program is the government-to-government method for selling US defense equipment, services, and training.

Mission Area: Special Mission Area (FY 2019: $238,553 thousand)

1. White House Communications Agency (WHCA) (FY 2019: $184,251 thousand): WHCA is a joint service military agency under the operational control of the White House Military Office (WHMO) and administrative control of the DISA. WHCA's mission is to provide information services to the President, Vice President, National Security Council, United States Secret Service and others as directed by WHMO ensuring the ability to communicate anywhere, anytime, by any means to anyone in the world, in accordance with Public Law 109-163. This support is provided in Washington, DC, worldwide travel sites, and second residences. Information services are also provided to the Presidential Information Technology Community. To meet its requirements, WHCA is structured to allow for fixed and travel (deployable) information services.

2. White House Situation Support Staff (WHSSS) (FY 2019: $17,733 thousand): The WHSSS was created by Presidential direction and provides classified communications, computer, and intelligence systems for the National Security Advisor, White House Situation Room, the National Security Council (NSC) staff, and other White House offices. WHSSS funds support the information systems used by the National Security Staff (NSS) and others. WHSSS provides upgrades and sustainment to the classified network systems used by the White House Situation Room and the NSC supporting the President, Vice President, National Security Advisor, and their staff.

I. Description of Operations Financed (cont.)

3. Crisis Management System (CMS) (FY 2019: $11,084 thousand): CMS is owned and operated by the National Security Staff (NSS) but maintained by DISA under the National Security Council direction and a National Security Decision Directive. The program provides state-of-the-art video teleconferencing (SVTS), facsimile, and the Executive Voice over Secure Internet Protocol (VoSIP) phone network (including the National Intelligence Watch Officers Network (NOIWON)) as directed by the NSS. The system functions in both fixed and mobile modes for exchange of time sensitive high interest information which extends the White House Situation Room presence. The system supports the President, National Security Council, Cabinet Members, Joint Chiefs, various agency watch centers, headquarters, and Continuity of Operations (COOP) sites.

Crisis Management System funding provides maintenance, configuration management, certification and accreditation activities including system security monitoring and testing, and engineering support. The system provides real-time Top Secret/Sensitive Compartmented Information (TS/SCI) secure video conference communications for the President and high level advisors including multi-party calls between fixed and mobile sites for day-to-day and crisis operations.

4. Minimum Essential Emergency Communications Network (MEECN) (FY 2019: $24,283 thousand): MEECN is a highly survivable communications capability which transmits Nuclear Command and Control (NC2) messages and establishes crisis conferences with the President, Vice President, Secretary of Defense, and the Chairman of the Joint Chiefs of Staff to the Commanders of the COCOMs and to deployed US nuclear forces. The DISA via the Strategic and National Command, Control, Communications, and Intelligence (SNC3I) Joint Systems Engineering and Integration Office (JSEIO) will support MEECN as the Nuclear Command, Control, and Communications (NC3) system engineer by providing architectures, performing systems engineering and analyses and assessments to support the

I. Description of Operations Financed (cont.)

C3 needs of national and senior government leadership. The NC3 System is composed of C3 assets that provide connectivity from the President and the Secretary of Defense through the National Military Command System (NMCS) to nuclear execution forces integral to fighting a "homeland-to-homeland," as well as theater, nuclear war. Additionally, the DISA will provide direct/indirect and specialized support to the DoD CIO and to the Joint Staff (JS), overarching technical and programmatic support recommendations for NC3 programs, as well as fail-safe procedures and risk reduction actions. DISA's efforts will assure and enable an informed decision making linkage between the President, the Secretary of Defense, and the Commanders of the Unified and Specified Commands to ensure proper C2 of our forces during times of stress and national emergency, up to and including nuclear war.

5. Communications Management Control Activity (CMCA) (FY 2019: $1,202 thousand): CMCA provides communications support to the United States Secret Service (USSS) for the presidential campaigns, as well as for dignitary protective duties. CMCA also supports the Joint Staff/J6, Joint Directorate of Military Support (JDOMS) for special events. Public Law 106-544 assigned USSS responsibility for coordinating, planning, exercising, and implementing security for National Special Security Events (NSSE). Additionally, DoD Directive 3025.13 mandated that DISA provide CMCA Headquarters with operations and maintenance funding.

II. Force Structure Summary:

N/A

III. Financial Summary ($ in thousands)

		FY 2018					
			Congressional Action				
A. BA Subactivities	FY 2017 Actuals	Budget Request	Amount	Percent	Appropriated	Current Estimate	FY 2019 Estimate
1. Transition to Net Centric Environment	122,458	140,281	0	0.0	0	140,281	233,443
2. Eliminate Bandwidth Constraints	258,974	239,688	0	0.0	0	239,688	217,754
3. DoDIN Network Operations and Defense	444,656	486,158	0	0.0	0	486,158	518,781
4. Exploit the DoDIN for Improved Decision Making	364,583	822,460	0	0.0	0	822,460	810,809
5. Deliver Capabilities Effectively/Efficiently	105,518	83,741	0	0.0	0	83,741	87,590
6. Special Missions	212,240	237,374	0	0.0	0	237,374	238,553
Total	**1,508,429**	**2,009,702**	**0**	**0.0**	**0**	**2,009,702**	**2,106,930**

* The FY 2017 Actual column includes $48,814.0 thousand of FY 2017 Overseas Contingency Operations (OCO) Appropriations Funding (PL 115-31).
* The FY 2018 Estimate column excludes $64,137.0 thousand of FY 2018 OCO Appropriations Funding.
* The FY 2019 Estimate column excludes $111,702.0 thousand of FY 2019 OCO Appropriations funding.

III. Financial Summary ($ in thousands)

B. Reconciliation Summary	Change FY 2018/FY 2018	Change FY 2018/FY 2019
Baseline Funding	**2,009,702**	**2,009,702**
Congressional Adjustments (Distributed)		
Congressional Adjustments (Undistributed)		
Adjustments to Meet Congressional Intent		
Congressional Adjustments (General Provisions)		
Subtotal Appropriated Amount	**2,009,702**	
Fact-of-Life Changes (2018 to 2018 Only)		
Subtotal Baseline Funding	**2,009,702**	
Supplemental	64,137	
Reprogrammings		
Price Changes		30,645
Functional Transfers		-50,720
Program Changes		117,303
Current Estimate	**2,073,839**	**2,106,930**
Less: Wartime Supplemental	-64,137	
Normalized Current Estimate	**2,009,702**	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
FY 2018 President's Budget Request (Amended, if applicable)		**2,009,702**
1. Congressional Adjustments		
a. Distributed Adjustments		
b. Undistributed Adjustments		
c. Adjustments to Meet Congressional Intent		
d. General Provisions		
FY 2018 Appropriated Amount		**2,009,702**
2. War-Related and Disaster Supplemental Appropriations		64,137
a. OCO Supplemental Funding		
1) FY18 OCO Funding	64,137	
3. Fact-of-Life Changes		
FY 2018 Baseline Funding		**2,073,839**
4. Reprogrammings (Requiring 1415 Actions)		
Revised FY 2018 Estimate		**2,073,839**
5. Less: Item 2, War-Related and Disaster Supplemental Appropriations and Item 4, Reprogrammings		-64,137
FY 2018 Normalized Current Estimate		**2,009,702**
6. Price Change		30,645
7. Functional Transfers		-50,720
a. Transfers In		
b. Transfers Out		
1) Multinational Information Sharing (MNIS) Program: A decrease of $-50,720 thousand and (-19) FTEs reflects the functional transfer of the Multinational Information Sharing (MNIS) Program responsibilities and resources from DISA to USAF to develop and field a Mission Partner Environment. (FY18 Baseline: $50,701 thousand)	-50,720	
8. Program Increases		185,980

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
a. Annualization of New FY 2018 Program		
b. One-Time FY 2019 Increases		
c. Program Growth in FY 2019		
1) Background Investigation IT Systems: National Background Investigation IT Systems (NBIS) will be in operation and production mode requiring system operations support, hardware/software repairs and Information Assurance Vulnerability Management (IAVM) updates. An increase of $66,657 thousand will sustain the following key capabilities: automated records checking, continuous evaluation, fingerprint and biometric processing, investigation adjudication, collection and validation of SF-86 data, designation of position sensitivity and integrated case management; provide key supporting infrastructure (e.g. data center hosting fees, government cloud, integration lab maintenance) and program management support. (FY18 Baseline: $50,154 thousand)	66,657	
2) Net-Centric Enterprise Services (NCES): An increase of $22,000 thousand supports application rationalization activities to modernize legacy applications and transition them to commercial or DoD cloud infrastructure. (FY18 Baseline: $40,667 thousand)	22,000	
3) Joint Service Provider (JSP) (4th Estate IT Onboarding): An increase of $20,000 thousand is attributed to additional requirements for Fourth Estate organizations that will require Joint Service	20,000	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
Provider (JSP) support. Additional scope of responsibility will include 200,000+ new users and will provide for network discovery, cyber posture reviews, and Command Cyber Readiness Inspections (CCRIs). (FY18 Baseline: $443,484 thousand)		
4) Information Systems Security Programs (ISSP)/Information Assurance (IA)/Public Key Infrastructure (PKI) - Joint Regional Security Stacks (JRSS):	16,732	
An increase of $16,732 thousand primarily funds the sustainment of Cyber Situational Awareness Analytic Capabilities (CSAAC) and support for Joint Regional Security Stacks (JRSS) migration. (FY18 Baseline: $222,720 thousand)		
5) Global Command and Control System-Joint (GCCS-J):	10,662	
An increase of $10,662 thousand primarily funds the modification of obsolete, high-security risk GCCS-J hardware needed to ensure compatibility with current industry standard hardware. The increase also provides additional maintenance releases for the Joint Planning and Execution Services (JPES) Framework. (FY18 Baseline: $91,628 thousand)		
6) Information Systems Security Programs (ISSP)/Information Assurance (IA)/Public Key Infrastructure (PKI):	10,028	
An increase of $10,028 thousand is primarily due to the purchase of ADP software licenses and lab equipment in support of the integration of Containment and EndPoint Detection and Response		

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
capabilities. Increase also provides hosting and engineering support to maintain and migrate engineering architecture review capabilities in support the NIPRNet and SIPRNet Cybersecurity Architecture Review (NSCSAR). (FY18 Baseline: $222,720 thousand)		
7) Combined Advanced Applications: Details provided for this program are submitted separately in appropriately classified DoD budget exhibits. (FY18 Baseline: $30,268 thousand)	7,195	
8) Compensation and Benefits (Shared Services): An increase of $4,985 thousand and (+38) FTEs primarily reflects an increase in non-technical support due to increased mission requirements throughout the Agency. These FTEs will consist of developmental level financial, acquisition and human resource analysts to compliment an aging workforce in these career fields. In addition, the increase reflects the realignment of non-major headquarters activities from Management Headquarters to Shared Services in order to comply with the Department's revised definitions of major headquarters activities and functions. (FY18 Baseline: $414,861 thousand)	4,985	
9) Joint Service Provider (JSP) (Rental Payments to GSA Leases): An increase of $4,861 thousand funds Joint Service Provider GSA leased space. Funding is realigned from equipment maintenance by contract for proper execution of funding. (FY18 Baseline: $443,484	4,861	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
thousand)		
10) Compensation and Benefits (Joint Service Provider (JSP)): An increase of $3,828 thousand and (+29) FTEs will fund additional IT specialists, computer scientists and engineers performing 24x7, secure and modern end-to-end IT services and architect and develop IT technology capabilities in the Pentagon and other locations within the National Capital Region (NCR). (FY18 Baseline: $414,861 thousand)	3,828	
11) Compensation and Benefits (Department of Defense Information Network Engineering Services (DODIN ES)): An increase of $3,740 thousand and (+29) FTEs is the result of the realignment from RDT&E to O&M. These FTEs will provide IT systems analysis, requirements analysis, cost analysis, and acquisition expertise to develop mission and business case analysis, and NIPRNet/SIPRNet Cyber Security Architecture Review (NSCAR) requirements for a quantitative analysis tool. (FY18 Baseline: $414,861 thousand)	3,740	
12) Joint Service Provider (JSP): An increase of $3,683 thousand is attributable to increased service support funding for the Joint Service Provider (JSP). The increase primarily provides funding for Pentagon Rent, security clearance processing, DFAS and audit support, disability compensation, mass transit benefits, and training not transferred by Army in the functional transfer. (FY18 Baseline: $443,484 thousand)	3,683	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
13) Pentagon Reservation Maintenance Revolving Fund (PRMRF):	3,134	
An increase of $3,134 thousand reflects the realignment of funding from equipment maintenance by contract to correctly align Joint Service Provider's Pentagon Rent costs to the proper cost category. (FY18 Baseline: $17,537 thousand)		
14) National Military Command System (NMCS):	2,103	
An increase of $2,103 thousand is primarily attributed to increased operational assessment requirements to provide National Leadership Command Capabilities (NLCC) architectural and engineering support. (FY18 Baseline: $4,801 thousand)		
15) Defense Information Systems Network (DISN) Enterprise Activities (EA):	1,500	
An increase of $1,500 thousand is due to support for the Airborne Intelligence Surveillance Reconnaissance (AISR) Integration team responsible for program planning, execution and sustainment support for AISR Transport capabilities. (FY18 Baseline: $147,007 thousand)		
16) Shared Service Units/Program Executive Offices:	1,238	
An increase of $1,238 thousand is primarily attributed to increased facility repairs, renovations, and general construction to the DISA Fort Meade, Maryland facility. (FY18 Baseline: $26,779 thousand)		
17) Compensation and Benefits (Change in Compensable Days):	1,237	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
Civilian personnel funding increases $1,237 thousand as a result of one more compensable workday in FY 2019 than in FY 2018. (FY18 Baseline: $414,861 thousand)		
18) Compensation and Benefits (Combined Advanced Applications): Details provided for this program are submitted in appropriately classified DoD exhibits submitted separately. (FY18 Baseline: $414,861 thousand)	828	
19) Field Commands and Field Offices: An increase of $794 thousand is primarily due to additional contractor support for country characterization assessments for the Critical Infrastructure Protection (CIP) program. (FY18 Baseline: $70,267 thousand)	794	
20) Department of Defense Information Network Engineering Services (DODIN ES): An increase of $505 thousand provides support services required to develop business cases and return on investments (ROI) analysis for enabling decision making. (FY18 Baseline: $46,239 thousand)	505	
21) Compensation and Benefits (Defense Information Systems Network (DISN) Enterprise Activities (EA)): An increase of $270 thousand and (+2) FTEs provide additional support for the Mobility Program's Morpheus Database and application development. (FY18 Baseline: $414,861 thousand)	270	
9. Program Decreases		-68,677
a. Annualization of FY 2018 Program Decreases		

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
b. One-Time FY 2018 Increases		
c. Program Decreases in FY 2019		
1) Senior Leadership Enterprise (SLE)/Logistics Support Activities (LSA): Details provided for this program are submitted separately in appropriately classified DoD budget exhibits. (FY18 Baseline: $167,630 thousand)	-22,248	
2) Defense Information Systems Network (DISN) Enterprise Activities (EA): A decrease of $-17,108 thousand is primarily due to the contract consolidation for maintenance of DoD Mobility Unclassified Capability (DMUC), DoD Mobility Classified Capability Secret (DMCC-S), and DoD Mobility Classified Capability Top Secret (DMCC-TS). (FY18 Baseline: $147,007 thousand)	-17,108	
3) DoD Teleport Program: A reduction of $-6,608 thousand is primarily due to decreased support requirements resulting from the completion of the Enhanced SATCOM Gateway Modem deployment. (FY18 Baseline: $29,601 thousand)	-6,608	
4) Joint Service Provider (JSP) (Realignment): A reduction of $-4,861 thousand in the equipment maintenance by contracts reflects a realignment to GSA leased space for proper execution of funding. (FY18 Baseline: $443,484 thousand)	-4,861	
5) Joint Service Provider (JSP): A decrease of $-3,400 thousand is due to the transfer of JSP funding from the DISA to the Office of the Secretary of Defense for the Principal Staff	-3,400	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
Assistants (PSA) to migrate, implement, and sustain the DoD NIPRNet-Demilitarized Zone (DMZ) efforts. (FY18 Baseline: $443,484 thousand)		
6) Net-Centric Enterprise Services (NCES): A decrease of $-2,440 thousand is primarily attributed to contract efficiencies achieved in the renewal of contracts for Enterprise Messaging and Identity Synchronization Services. (FY18 Baseline: $40,667 thousand)	-2,440	
7) Network Operations (NetOps): A decrease of $-2,429 thousand and reduced contract support is primarily due to the loss of one shift per day as the boundary defense for the DoD goes from a 24x7 to 16x7 operation. (FY18 Baseline: $122,065 thousand)	-2,429	
8) Defense Information Systems Network (DISN) Infrastructure Services (DISN-IS): A decrease of $-2,291 thousand is primarily due to reduced Global Video Services (GVS) and Global Video Desktop Services (GVDS) requirements. (FY18 Baseline: $24,793 thousand)	-2,291	
9) Compensation and Benefits (Management Headquarters): A decrease of $-2,240 thousand and (-14) FTEs reflects the realignment of non-major headquarters activities from Management Headquarters to Shared Services in order to comply with the Department's revised definitions of major headquarters activities and functions. (FY18 Baseline: $414,861 thousand)	-2,240	
10) Minimum Essential Emergency Communications Network	-2,130	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
(MEECN): A decrease of $-2,130 thousand is attributed to decreased operational assessment requirements to execute National Leadership Command Capabilities (NLCC) architectural and engineering. (FY18 Baseline: $26,029 thousand)		
11) Defense Spectrum Organization (DSO): A decrease of $-1,185 thousand is primarily due to the transition of services to MILCLOUD, requiring less contractor support. (FY18 Baseline: $37,078 thousand)	-1,185	
12) Joint Staff Support Center (JSSC): A decrease of $-887 thousand is due to anticipated reductions in HVAC requirements. (FY18 Baseline: $26,384 thousand)	-887	
13) Global Combat Support System-Joint (GCSS-J): A decrease of $-430 thousand is due to reduced hardware maintenance costs as GCSS-J transitions to a virtual environment. (FY18 Baseline: $16,989 thousand)	-430	
14) Defense Industrial Base (DIB): Details provided for this program are submitted separately in appropriately classified DoD budget exhibits. (FY18 Baseline: $9,535 thousand)	-178	
15) Crisis Management System (CMS): A decrease of $-177 thousand is primarily attributed to the elimination of a CMS circuit. (FY18 Baseline: $11,085 thousand)	-177	
16) Management Headquarters:	-65	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
A decrease of $-65 thousand is primarily due to a reduction in court reporter services due to reduced litigation. (FY18 Baseline: $39,051 thousand)		
FY 2019 Budget Request		**2,106,930**

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
Net-Centric Enterprise Services (NCES):			
1. Customer usage/satisfaction -- Receive an overall customer usage/satisfaction rating ≥ 3 on a scale of 1 to 5 where 1 is "no mission effectiveness", 3 is "supports mission effectiveness and is relevant to evolving mission needs", and 5 is "maximum mission effectiveness".	1. Met	1. ≥ 3	1. ≥ 3
2. Availability -- Operational enterprise services sustain the customer requirement of ≥ .997 availability/reliability	2. Met	2. ≥ .997	2. ≥ .997
Department of Defense Information Network Engineering Services (DODIN ES):			
1. Maintain at least 25% spare capacity, to allow for provisioning of unforeseen requirements and rerouting under outages.	1. Met	1. ≥ 25%	1. ≥ 25%
2. Total number of engineering artifacts adopted greater than 5.	2. Met	2. ≥ 5	2. ≥ 5

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
National Background Investigation Services (NBIS):			
1. FTE Percentage: Establishment and full staffing of the PMO.	1. 90%	1. 100%	1. N/A
Standardized Tactical Entry Point (STEP):			
1. STEP Resource Availability: Probability that STEP resources are operable or usable to perform it's designated or required function (ratio of time the system is functional). Target is no more than 8 hours, 45 minutes, and 36 seconds of downtime or service interruptions per year.	1. Met	1. ≤ 8 hours, 45 minutes, and 36 seconds	1. ≤ 8 hours, 45 minutes, and 36 seconds
2. STEP Reliability: Probability that STEP will accurately perform its specified task under stated environmental conditions (ability of the system to perform consistently to its design). Target is no more than 8 hours, 45 minutes, and 36 seconds of downtime or service interruptions per	2. Met	2. ≤ 8 hours, 45 minutes, and 36 seconds	2. ≤ 8 hours, 45 minutes, and 36 seconds

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
site per year.			
DoD Teleport Program: Teleport system availability -- Utilizing two-in-view architecture, maintain 99% of global availability of Teleport systems.	1. Met	1. 99%	1. 99%
Defense Information Systems Network (DISN) Enterprise Activities (EA): 1. Enhanced Pentagon Capability/Survivable Emergency Conferencing Network (EPC/SECN): Ensure that EPC/SECN resources are operable or usable to perform their designated or required function at a targeted level of 99.99% without system interruption or downtime.	1. Met	1. ≥ 99.0%	1. ≥ 99.0%
2. Defense Satellite Communications system (DSCS/Global SATCOM Support Center (GSSC) Support Element. To support approved mission requests (100% completion)at a targeted level of 99.99%. An	2. Met	2. ≥ 99.0%	2. ≥ 99.0%

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
"approved mission request" is a Satellite Access Request (SAR).			
Defense Information Systems Network (DISN) Infrastructure Services:			
1. Non-Secure Internet Protocol Network (NIPRNet) access circuit availability. Target: ≥ 98.50%	1. Met	1. ≥ 98.50%	1. ≥ 98.50%
2. Secure Internet Protocol Router Network (SIPRNet) latency (measurement of network delay). Target: Not to exceed 100 Milliseconds	2. Met	2. ≤ 100 Milliseconds	2. ≤ 100 Milliseconds
3. Defense Red-Switch Network (DRSN) switch availability.	3. NA	3. ≥ 99.99%	3. ≥ 99.99%
Network Operations (NetOps):			
1. Percent SATCOM network fully operational -- Conduct operational management of all apportioned and non-apportioned DISA Satellite Communications (SATCOM)/Gateway resources to ensure full service	1. Met	1. 99.9%	1. 99.9%

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
reliability and availability of the SATCOM network for our customers. Target is to maintain 99.9% of service availability at all times to the user.			
2. Number of Mission Denials -- Global Tactical Mission Manager and Gateway Service Desk (GSD) plan and support missions entering 16 DoD Gateways. Target is less than 1% per year.	2. Met	2. < 1% per year	2. < 1% per year
3. JFHQ-DODIN synchronizes forces to harden the DODIN.			
a. % of task orders completed	3a. N/A	3a. 85%	3a. 85%
b. % of planned COCOM CONPLAN and OPLAN defensive cyber support plans completed	3b. 100%	3b. 85%	3b. 85%

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
Information Systems Security Program (ISSP)/Information Assurance (IA)/Public Key Infrastructure (PKI):			
1. PKI -- Certificate Revocation Status. Target: < 5 seconds	1. < 3 seconds	1. < 5 seconds	1. < 5 seconds
2. CMRS -- How many new user accounts with defined permissions were created in the past 30 days? (NIPR & SIPR) Target: 50	2. 50	2. 50	2. 50
3. CSAAC Analytics -- Number of OPT Sensors Deployed/Maintained. Target: 9000	3. 9000	3. 9000	3. 9000
4. JRSS -- Implement JMS CSAAC analytic capability at 12 JRSS locations by FY 2018.	4. 11	4. 1	4. N/A
Field Commands and Field Offices:			
1. Bring DISA exercise programs into full compliance with Joint Staff Standards. Target is the number	1. 10	1. 5	1. 5

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
COCOM Tier 1 exercises in full compliance with Joint Staff Standards (FY16 Measurable Target: 5 exercises).			
2. Leverage CIP programs to identify risk and mitigation strategies. FY16 Target is 22 mitigation strategies reviewed/ developed.	2. 30	2. 22	2. 22
Joint Staff Support Center (JSSC):			
1. JSSC provides over 250 thousand patches per year for NC, & C2 Systems and 12 thousand patches per year for Video, Graphic, Intel and VTC products. Target is 100% resolution of all incidents; elevate incidents to program manager as required. Target is 100% resolution of all incidents.	1. Met	1. 100%	1. 100%
2. IT Support for over 1000 Nuclear Decision Conferences and over 600 Worldwide GCCS-J/JOPES/ SORTS sites. Target is to maintain 99% of global availability of critical sites world-wide and 24x7 monitoring and reporting of GCCS-J and NCCS systems	2. Met	2. 100%	2. 100%

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
status, and operational impacts.			
White House Situation Support Staff (WHSSS): 1. 99.9% uptime availability of classified networks, phones and peripherals in support of the WH Situation Room and NSC	1. Met	1. 99.0%	1. 99.0%
2. Ensure 99.9% network uptime for COOP and COG facilities.	2. Met	2. 99.9%	2. 99.9%
Minimum Essential Emergency Communications Network (MEECN): 1. Product Delivery -- Provide engineering products in all task areas that satisfy customer needs at least 90% of the time.	1. Met	1. 90%	1. 90%
2. Systems Assessments -- Conduct assessments of the Nuclear C3 system and the SLC3S that provide actionable results and recommendations for the Joint Staff and OSD/CIO to pursue improvements to these capabilities at least 90% of the time.	2. Completed 90% of scheduled assessments	2. Assessments conducted 90% of the time	2. Assessments conducted 90% of the time

IV. Performance Criteria and Evaluation Summary:

Metric Description by Program	2017 Actual	2018 Plan	2019 Plan
3. Reliability -- 98.9% availability of the DISA-managed infrastructure.	3. Met	3. 98.9%	3. 98.9%
Communications Management Control Activity (CMCA): Service Availability -- The performance will be measured based on maintaining 99.9% availability of the CATT tool to the authorized users in a reliable, responsive, and timely manner at all times.	1. Met	1. 99.9%	1. 99.9%

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2019 President's Budget

V. Personnel Summary	FY 2017	FY 2018	FY 2019	Change FY 2017/ FY 2018	Change FY 2018/ FY 2019
Active Military End Strength (E/S) (Total)	1,320	1,668	1,661	348	-7
Officer	322	381	375	59	-6
Enlisted	998	1,287	1,286	289	-1
Reserve Drill Strength (E/S) (Total)	14	15	15	1	0
Officer	1	1	1	0	0
Enlisted	13	14	14	1	0
Civilian End Strength (Total)	2,512	3,116	3,223	604	107
U.S. Direct Hire	2,454	3,019	3,090	565	71
Total Direct Hire	2,454	3,019	3,090	565	71
Reimbursable Civilians	58	97	133	39	36
Active Military Average Strength (A/S) (Total)	1,320	1,668	1,661	348	-7
Officer	322	381	375	59	-6
Enlisted	998	1,287	1,286	289	-1
Reserve Drill Strength (A/S) (Total)	14	15	15	1	0
Officer	1	1	1	0	0
Enlisted	13	14	14	1	0
Civilian FTEs (Total)	2,436	3,116	3,223	680	107
U.S. Direct Hire	2,383	3,019	3,090	636	71
Total Direct Hire	2,383	3,019	3,090	636	71
Reimbursable Civilians	53	97	133	44	36
Average Annual Civilian Salary ($ in thousands)	147.9	137.4	138.2	-10.5	.8
Contractor FTEs (Total)	3,308	4,098	4,173	790	75

FY 2017-2018: The FTE change from FY 2017 - FY 2018 is (+680) FTEs. The FTE change is due to the following:

Functional Transfer (+462) FTEs: An increase of (+462) FTEs reflects the functional transfer from the Army Information Technology Agency (ITA) (+247), Washington Headquarters Services (WHS) Enterprise Information Technology Services Directorate (EITSD) (+169), and the Joint Staff Director of IT Services (+46) to DISA as a result of the consolidation of IT services in the Pentagon and National Capital Region (NCR).

Departmental Adjustments (+51) FTEs: An increase of (+44) FTEs provides for engineering, network, and White House IT helpdesk support required to successfully field and sustain the Presidential Information Technology Community (PITC) mission. An increase of (+5) FTEs provides IT Engineers to support the modernization of endpoint security on DoD networks and to implement pilot and test security solutions within the DODIN. The Joint Service Provider (JSP) program increases (+2) FTEs. Details provided for this program are submitted separately in appropriately classified DoD budget exhibits.

DISA Internal Adjustments (+141) FTEs: An increase of (+141) FTEs is due to increased hiring actions to fill vacancies created from retirements and attrition in FY 2017.

Management Headquarters Reduction (-18) FTEs: A (-18) FTE reduction is primarily attributed to a DoD efficiency reduction in management headquarters staffing.

Reimbursable Workload: An increase of (+44) FTEs is due to an increase in anticipated reimbursable workload.

FY 2018-2019: The FTE change from FY 2018 - FY 2019 is (+107) FTEs. The FTE change is due to the following:

DISA Internal Adjustments (+84) FTEs: An increase of (+38) FTEs primarily reflects an increase in non-technical support due to increased mission requirements throughout the Agency. These FTEs will consist of developmental level financial, acquisition and human resource analysts to compliment an aging workforce in these career fields. In addition, the increase reflects the realignment of non-major headquarters activities from Management Headquarters to Shared Services in order to comply with the Department's revised definitions of major headquarters activities and functions. An increase of (+29) FTEs is the result of the realignment from RDT&E to O&M. These FTEs will provide IT systems analysis, requirements analysis, cost analysis, and acquisition expertise to develop mission and business case analysis, and NIPRNet/SIPRNet Cyber Security Architecture Review (NSCAR) requirements for a quantitative analysis tool. An increase of (+29) FTEs for the Joint Service Provider (JSP) will fund additional IT specialists, computer scientists and engineers to perform 24x7, secure and modern end-to-end IT services and architect and develop IT technology capabilities in the Pentagon and the National Capital Region (NCR). An increase of (+2) FTEs provide additional support for the Mobility Program's Morpheus Database and application development. A (-14) FTE decrease reflects the realignment of non-major headquarters activities from Management Headquarters to Shared Services in order to comply with the Department's revised definitions of major headquarters activities and functions.

Departmental Adjustments (+6) FTEs: The Combined Advanced Application Program increases (+6) FTEs. Details provided for this program are submitted in appropriately classified DoD exhibits submitted separately.

Functional Transfer (-19) FTEs: A decrease of (-19) FTEs reflects the functional transfer of the Multinational Information Sharing (MNIS) Program responsibilities and resources from DISA to USAF to develop and field a Mission Partner Environment.

Reimbursable Workload (+36) FTEs: An increase of (+36) FTEs establishes the reimbursable manpower required for the Joint Service Provider (JSP) Telecommunication Program.

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

OP 32 Line	FY 2017 Actuals	Change FY 2017/FY 2018 Price	Change FY 2017/FY 2018 Program	FY 2018 Estimate	Change FY 2018/FY 2019 Price	Change FY 2018/FY 2019 Program	FY 2019 Estimate
101 Exec, Gen'l & Spec Scheds	352,344	6,885	55,632	414,861	2,116	9,989	426,966
107 Voluntary Sep Incentives	16	0	-16	0	0	0	0
199 Total Civ Compensation	**352,360**	**6,885**	**55,616**	**414,861**	**2,116**	**9,989**	**426,966**
308 Travel of Persons	36,237	616	-6,087	30,766	554	-224	31,096
399 Total Travel	**36,237**	**616**	**-6,087**	**30,766**	**554**	**-224**	**31,096**
671 DISA DISN Subscription Services (DSS)	25,643	487	20,196	46,326	834	-994	46,166
672 PRMRF Purchases	18,071	-92	-124	17,855	-109	3,134	20,880
677 DISA Telecomm Svcs - Reimbursable	0	0	43,720	43,720	831	-5,959	38,592
696 DFAS Financial Operation (Other Defense Agencies)	7,658	-93	-1,395	6,170	318	0	6,488
699 Total DWCF Purchases	**51,372**	**302**	**62,397**	**114,071**	**1,874**	**-3,819**	**112,126**
771 Commercial Transport	2,345	40	1,805	4,190	75	0	4,265
799 Total Transportation	**2,345**	**40**	**1,805**	**4,190**	**75**	**0**	**4,265**
901 Foreign National Indirect Hire (FNIH)	41	1	-42	0	0	0	0
912 Rental Payments to GSA (SLUC)	1,165	20	835	2,020	36	4,862	6,918
913 Purchased Utilities (Non-Fund)	3,909	66	7,382	11,357	204	-887	10,674
914 Purchased Communications (Non-Fund)	29,575	503	7,917	37,995	684	-308	38,371
915 Rents (Non-GSA)	78	1	50	129	2	0	131
917 Postal Services (U.S.P.S)	12	0	204	216	4	0	220
920 Supplies & Materials (Non-Fund)	9,446	161	-1,011	8,596	155	0	8,751
921 Printing & Reproduction	27	0	62	89	2	0	91
922 Equipment Maintenance By Contract	885,079	15,047	280,412	1,180,538	21,250	39,091	1,240,879
923 Facilities Sust, Rest, & Mod by Contract	12,241	208	-5,004	7,445	134	1,151	8,730
925 Equipment Purchases (Non-Fund)	48,091	818	-10,203	38,706	697	619	40,022
932 Mgt Prof Support Svcs	351	6	1,357	1,714	31	0	1,745

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2019 President's Budget

OP 32 Line	FY 2017 Actuals	Change FY 2017/FY 2018 Price	Change FY 2017/FY 2018 Program	FY 2018 Estimate	Change FY 2018/FY 2019 Price	Change FY 2018/FY 2019 Program	FY 2019 Estimate
933 Studies, Analysis & Eval	877	15	1,285	2,177	39	0	2,216
934 Engineering & Tech Svcs	470	8	1,164	1,642	30	0	1,672
957 Other Costs (Land and Structures)	43	1	-44	0	0	0	0
987 Other Intra-Govt Purch	18,682	318	38,762	57,762	1,040	2,580	61,382
989 Other Services	56,028	952	38,448	95,428	1,718	13,529	110,675
999 Total Other Purchases	**1,066,115**	**18,125**	**361,574**	**1,445,814**	**26,026**	**60,637**	**1,532,477**
Total	**1,508,429**	**25,968**	**475,305**	**2,009,702**	**30,645**	**66,583**	**2,106,930**

* The FY 2017 Actual column includes $48,814.0 thousand of FY 2017 Overseas Contingency Operations (OCO) Appropriations Funding (PL 115-31).
* The FY 2018 Estimate column excludes $64,137.0 thousand of FY 2018 OCO Appropriations Funding.
* The FY 2019 Estimate column excludes $111,702.0 thousand of FY 2019 OCO Appropriations funding.