Fiscal Year (FY) 2008/FY 2009 Budget Estimates
Defense Information Systems Agency (DISA)

February 2007

(This page intentionally left blank.)

DEFENSE INFORMATION SYSTEMS AGENCY
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2008/FY 2009 Budget Estimates

Operation and Maintenance, Defense-Wide Summary ($ in thousands)
Budget Activity (BA) 4: Administrative and Service-Wide Support

	FY 2006 Actuals*	Price Change	Program Change	FY 2007 Estimate**	Price Change	Program Change	FY 2008 Estimate	Price Change	Program Change	FY 2009 Estimate
DISA	1,160,139	29,478	(208,724)	980,893	23,256	(58,555)	945,594	22,091	150,323	1,118,008

* The FY 2006 Actual column includes $2.744 thousand of Hurricane Supplemental funds (PL 108-324, PL 109-61, and PL 109-62), $77.000 thousand of Iraq Freedom Fund transfers, and $40.000 thousand of FY 2006 Title IX obligations (PL 108-287).
** The FY 2007 Estimate column excludes $38.800 million of FY 2007 Title IX, Global War on Terrorism (PL 109-289), but includes $21.700 thousand for Spectrum Relocation Fund (P.L. 108-494).

I. Description of Operations Financed:

The Defense Information Systems Agency (DISA) is the combat support agency that plans, engineers, acquires, fields, and supports global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, warfighters and other DoD Components, under all conditions of peace and war. The DISA provides telecommunications and information technology services common to the DoD components more effectively, economically, and efficiently than they could do individually. In support of the DOD goals for net-centricity and interoperability, the DISA provides products and leads activities that enable jointness. The DISA envisions a world in which information is virtual and on demand with global reach. Information is protected by identity-based capabilities that allow users to connect, be identified, and access needed information in a trusted manner. It is a world in which United States military forces can deploy and connect no matter where they are located, pull information needed for their missions, and be given timely, accurate information on any threats they may face. It is a world with no seams between the sustaining base and the tactical edge that enables operational agility. It is a world in which the United States military can freely exchange information routinely with coalition partners and others responsible for the security and defense of the United States.

I. Description of Operations Financed (continued):

The DISA operates under the direction, authority, and control of the Assistant Secretary of Defense (Networks and Information Integration (ASD (NII)). The DISA's responsibilities include:

- Providing secure Joint Command, Control, Communications, and Computer Systems in support of peacetime, contingency, war or other crisis;
- Supporting contingency and wartime planning with the Joint Staff and the Combatant Commands (CoCOM);
- Maintaining effective communications for deployed elements in Afghanistan, Kuwait, Qatar, and Iraq in support of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF);
- Acting as a force provider for USSTRATCOM Joint Force Headquarters-Information Operations, with responsibilities for global network operations and network defense capabilities;
- Providing support for Senior Leadership Communication capabilities for the President and Vice President, the Secretary of Defense and other DoD executives;
- Providing network-centric enterprise services for the Global Information Grid (GIG) in the form of applications and services;
- Providing enterprise-wide computing services for DoD;
- Supporting Joint Exercises;
- Supporting Homeland Defense in cases of natural disaster, terrorism and other contingencies, such as the Hurricane Katrina event;

I. Description of Operations Financed (continued):

- Protecting the Global Information Grid (GIG), including telecommunications, information systems, and information technology that processes unclassified, sensitive and classified data;
- Providing electromagnetic spectrum access to meet DOD's global mission, and providing planning, international spectrum coordination, and other spectrum management services;
- Maintaining human resource initiatives to retain and reshape the DISA's workforce to meet future requirements, increase quality and technical depth, and support upcoming challenges.

DISA is organized and structured in support of DOD's strategic framework; to incorporate the goals and objectives in the President's Management Agenda; to address customer requirements and priorities; and to implement the DoD and the DISA Balanced Scorecard strategies. The most relevant DoD priorities include: (1) successfully pursue the Global War on Terrorism; (2) strengthen joint and combined warfighting capabilities; (3) transform the Joint Force; and (4) streamline DoD processes.

DISA aligns its mission, essential tasks, goals and strategies, and program resource structure across six mission areas. These mission areas reflect the DoD goals and represent the DISA's focus on key activities. Subsequent sections provide detailed descriptions of the mission areas:

1. Transition to a net-centric environment to transform the way DoD shares information by making data continuously available in a trusted environment.

I. Description of Operations Financed (continued):

2. Build and sustain the GIG transport infrastructure that eliminates bandwidth constraints and rapidly surges to meet demands, whenever and wherever needed.

3. Operate, manage, and defend the GIG to enhance critical warfighting and business capabilities in a secure, net-centric environment.

4. Transition to DoD enterprise-wide capabilities for communities of interest, e.g. command and control, combat support, that exploit the GIG for improved decision-making.

5. Deliver capabilities, based on established requirements, more effectively, economically, and efficiently, than we do today.

6. 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.

The first five categories reflect the customer support strategies of the DISA Balanced Scorecard, the sixth category represents the DISA's critical special mission to support the Commander in Chief.

Significant Program Changes:

The FY 2008 budget reflects on-going DISA activities in the context of their support to the Secretary of Defense's strategic direction. The following programs reflect significant changes:

I. Description of Operations Financed (continued):

Net-Centric Enterprise Services (NCES): NCES increases sustainment efforts of the various NCES capabilities. Milestone C is scheduled to occur in FY 2008 with Initial Operational Test and Evaluation (IOT&E) occurring late in FY 2008. NCES Initial Operating Capability (IOC) will reach full operability by FY 2009 as evident in NCES core enterprise services migrating to sustainment for Service Oriented Architecture Foundation, Content Discovery and Delivery, Enterprise Collaboration, and Enterprise Portal. The NCES System Development and Demonstration Phase will completely transition into the Production Phase following the Full Deployment Decision Review by the end of FY 2008.

Information Systems Security Program (ISSP)/Information Assurance (IA): The DISA continues to focus on designing and deploying proactive protections, deploying attack detection, and performing Information Assurance (IA) operations to ensure that adequate security is provided. Beginning in FY 2008 ISSP/IA will implement host-based security systems at the enterprise level. This will include content filtering and intrusion prevention on secure networks and internet gateways as well as network access controls for classified networks.

Global Command and Control System – Joint (GCCS-J): The DISA is executing functional transfers to the Joint Staff Support Center (JSSC) local mission funding from the GCCS-J to the National Military Command System (NMCS) program element, and the legacy Common Operating Environment sustainment activities into the GCCS-J program element from the GIG Engineering Services program element.

Defense Spectrum Organization (DSO): The DSO will transform the DOD's legacy spectrum management processes and capabilities to support an emerging net-centric environment in which radio frequency-based resources play an integral role. DSO funding

I. Description of Operations Financed (continued):

declines in FY 2008 following the transfer of $21.7 million to the DISA for DOD Spectrum Relocation Fund activities in FY 2007.

White House Communications Activity (WHCA): The WHCA is a joint service military agency under the operational control of the White House Military Office (WHMO) and the administrative control of the DISA. The WHCA will focus its efforts in FY 2008 and FY 2009 on sustaining and refreshing communications support to the White House. The WHCA will sustain the fixed and travel missions at the high OPTEMPO levels expected in FY 2008, modernize Presidential secure communications systems to correct shortfalls in reliability and voice quality; upgrade video distribution at Presidential facilities to digital in advance of the FCC-mandated analog TV phase-out; provision communications at the next Presidential and Vice-Presidential second residences, and complete the relocation of critical communications nodes to a location outside the Washington area. In addition, the WHCA will improve quality and reliability of non-secure voice communications for the President and supporting staff, expand Presidential support staff's access to intelligence data, improve the Presidential support data network's reliability and survivability, and evaluate off-the-shelf solutions for Presidential communications requirements.

- Key DOD/DISA initiatives reflected in this budget submission include:
- Support for force provider responsibilities maintaining USSTRATCOM Global Network Operations and Defense missions assigned by the Secretary of Defense;
- Support to the CoCOM equipment upgrades for the Combined Enterprise Regional Information Exchange System (CENTRIXS) program;

I. Description of Operations Financed (continued):

- Expansion of Computer Network Defense improvements for Computer Emergency Response Teams, expanding SIPRNet protection capabilities, and countering Insider Threat activities;
- Continued use of the DISA Total Cost Allocation Model that assigns costs of shared services to products and services; to identify the total cost of a program; to avoid unintended subsidy to the Defense Working Capital Fund and gain visibility and insight into cost and consumption of shared services and address efficiencies.

I. Description of Operations Financed: By Mission Area

1. Transition to Net Centric Environment: The ability to conduct network-centric operations is central to Department's warfighter and business transformation. Reducing investment in legacy enterprise programs (Information Dissemination Management (IDM) and Defense Collaboration Tool Suite (DCTS)) provided increased funding for Net-Centric Enterprise Services (NCES) in preparation for fielding of Increment One capabilities in FY 2008. Funding for the Global Information Grid Engineering Services reflects increased support to Net-Centric Systems Engineering processes. The budget reflects a slight decrease to Advanced Information Technology Services for Advanced Concept Technology Demonstrations and decreased funding to the Coalition Warrior Interoperability Demonstration. The following programs comprise the Transition to Net Centric Environment mission area:

I. Description of Operations Financed (continued): By Mission Area

Mission Area Component ($ in Thousands)	FY 2006 Actuals	FY 2007	FY 2008	FY 2009
a. Net-Centric Enterprise Services	22,780	28,013	28,969	86,867
b. Global Information Grid Engineering Services	52,076	57,454	55,828	70,983
c. Defense Collaboration Tool Suite	10,733	0	0	0
d. Advanced Information Technology Services	8,548	6,238	6,355	7,295
e. Coalition Warrior Interoperability Demonstration	2,049	1,102	2,187	2,267
f. Information Dissemination Management	15,249	0	0	0
Transition to Net Centric Environment Total	**111,435**	**92,807**	**93,339**	**167,412**

a. Net-Centric Enterprise Services (NCES)

The Net-Centric Enterprise Services (NCES) vision is to enable the secure, agile, robust, dependable, and interoperable data sharing environment for the Department of Defense (DoD) where the warfighter, business, and intelligence users share information on a global network that facilitates information superiority, accelerated decision-making, effective operations, and net-centric transformation. Data is an essential enabler of network-centric warfare. As the DoD Components implement DoD 8320.2, “Data Sharing in a Net-Centric Department of Defense,” data will be made visible, accessible and understandable to other potential users by metadata (“tagging”), web-service enabling, and registering of metadata. NCES services are essential for making that data useful to others within the enterprise. NCES enables the DoD to fully leverage the value of its information by providing discovery and accessing of data.

I. Description of Operations Financed (continued): By Mission Area

The operational benefits enabled by NCES include:

1. Increased speed of command and greater precision of desired effects resulting from shared situational awareness and informed decision-making.

2. Improved interoperability resulting from the use of shared services and authoritative data that is timely, understandable, complete, and available to all users.

3. Enhanced information superiority, with the objective to achieve enhanced decision superiority through an increase in the availability of relevant and authoritative information.

4. Increased agility enabled by the improvement in machine-to-machine interactions reducing the need for human intervention and reduced footprints resulting from greater ability to access information and services regardless of where they reside.

5. An improved ability to conduct planning and support of coordinated execution at multiple echelons (National, Strategic, Operational, and Tactical) in a nearly parallel fashion using the concepts of shared spaces and common collaboration and decision support tools.

6. An improved security posture providing dynamic, continual security measures, and ensuring identity, data authenticity, and secure communications.

The NCES supports the DoD’s transformation goals to achieve rapid decision superiority, to streamline business processes, and to conduct effective and discriminate information

I. Description of Operations Financed (continued): By Mission Area

operations. The NCES transforms legacy planning and execution capabilities into protected, web-based, real-time collaborative business processes, including Joint and Coalition information exchanges across organizational boundaries. NCES meets the military requirement to provide dramatically improved situational awareness, robust alerting, shortened decision cycles, and shared understanding.

NCES Increment I will eliminate costly legacy interfaces among disjointed, disparate, and stove-piped systems by providing a comprehensive set of nine (9) interoperable core enterprise services. These nine (9) core enterprise services are:

(1) Collaboration: this service will enable real-time situational updates to time critical planning activities among joint, coalition partners, the intelligence community, and Agencies at all levels (DoD, Federal, State, and Local) and provide real-time information sharing and processing anywhere and anytime, by any user with privileges on the DoD network. Collaboration includes being able to see, hear, and talk to all participants in a collaborative session; securely share files, information, and applications stored on local computers; and make presentations to large or small audiences;

(2) Mediation: this service will enable users to translate data from one format to another so that the data can be used by all users no matter what format they prefer. This service increases data interoperability and enables all warfighting and business users to be able to communicate with each other to support rapid decision-making;

(3) Information Assurance/Security (IAS): This service provides authentication, access management, and domain security services. These security services enable resistance to non-user system access and interference, in addition to preventing user misuse and

I. Description of Operations Financed (continued): By Mission Area

security errors. The security service interoperates with the other core services to protect the NCES as a whole entity. This service relies on the Public Key Infrastructure (PKI) and supports user authentication and validation services;

(4) Discovery: the enabling of all users no matter where they are to find the necessary information required to do their jobs faster and make better decisions faster. This service includes finding services provided by other DoD programs for users with the proper credentials to have access to (Service Discovery), finding people logged onto the network and any devices connected to the network (People and Device Discovery), finding all types of web content, and data distributed throughout DoD;

(5) Enterprise Services Management (ESM): this service provides the ability to monitor, manage, and scale web services appropriately, thereby assuring that the NCES services are available to the user whenever the user needs it. Enterprise Services Management (ESM) will also provide performance monitoring, mission impact assessment, and problem detection and resolution to make sure that the user is getting information and services in ways that are useful;

(6) Storage: this service provides the necessary storage to deliver the necessary content and information to the users. Warfighter, Business, and Intelligence communities are developing and maintaining enough information that will push today's storage limitations beyond their current capabilities. Hence, NCES provides enough storage capacity to support current and future needs. The NCES provides a storage architecture, storage operations, capacity management, and storage policies and procedures;

(7) Application: this service will provide a protected hosting environment consisting of common hardware platforms and operating systems. This is the infrastructure where all

I. Description of Operations Financed (continued): By Mission Area

NCES services and applications will reside within a Defense Enterprise Computing Center. Users will be able to access NCES services no matter where they are, thereby supporting mobile decision making;

(8) Messaging: this service provides secure machine to machine communications on behalf of the user, provide various notifications and alerts, and interoperable global communications support. In summary, all the mechanisms for delivering content efficiently and reliably across the enterprise; and

(9) User Assistant: this service provides users with help desk services, automated helper assistants, and enables the user the ability to customize the way they want to interact with NCES.

These nine (9) Core Enterprise Services are grouped and implemented as four (4) product lines:

1. Service Oriented Architecture (SOA) Foundation,
2. Content Discovery and Delivery (CD&D),
3. Enterprise Collaboration, and
4. Enterprise Portal.

The SOA Foundation provides the ESM, Mediation, Messaging, Information Assurance/Security, finding services provided by DoD programs (Service Discovery), and finding people or devices (People and Device Discovery). The CD&D provides the Google™ like functionality of finding web content, storage, and delivering that content to the users. The DKO Portal represents a way for users to get access to the services provided by NCES and provides all the tools associated with the User Assistant core enterprise

I. Description of Operations Financed (continued): By Mission Area

service. The DoD Enterprise Collaboration will provide users with a range of capabilities, such as chat, web conferencing, application sharing, white boarding including annotations, and application broadcasting that meets DoD security and operational requirements. These four (4) product lines will be provided and supported throughout the full life cycle by managed service providers who will offer their services from a qualified Global Information Grid Computing Node.

The SOA Foundation services product line offers interoperable net-centric services that enable programs across the DoD to share services-based applications and information across the GIG, which results in a reduction in cost and development effort. The core services for the SOA Foundation include information assurance/service security, service discovery, enterprise service management, machine-to-machine messaging, mediation, metadata discovery, and people and device discovery.

The Content Discovery and Delivery services product line is essential in the DoD infrastructure to provide common specifications to expose, search, retrieve, and deliver information across the enterprise. CD&D provides the methodology, specifications, user interfaces, and services to support discovery, and efficient delivery of information. CD&D services provide the capability to perform federated search, enterprise catalog, data source integration, and enterprise delivery of content.

The DoD Enterprise Collaboration service product line collaboration and messaging capabilities such as white board and conferencing sessions, messaging and a variety of collaboration tools, i.e., session management, presence and awareness, audio, video, text, annotation, application sharing and broadcasting, and virtual spaces. An enclave solution for the Collaboration service is also provided separately to coalition partners

I. Description of Operations Financed (continued): By Mission Area

since they operate on separate secure networks and are not connected to the SIPRNet or NIPRNet.

The Defense Knowledge Online Portal product line provides a personalized, user-defined, web-based presentation that allows for secure access to various enterprise services, including retrieval and posting of information, collaboration tools, instant messaging, and workgroups. The DKO Portal also integrates with security services for increased security and administration. The DKO Portal provides end user access to NCES services as well as providing a platform to launch NCES services directly from customer owned portals. The DKO Portal has several fundamental features, including a single sign on access point, Find, and Metadata Discovery.

The NCES Product services will support both information sharing and shared situational awareness of the discovery, collaboration, mediation, and messaging environments. The NCES services will link decision makers and system users with current, essential data to achieve increased speed of command.

Operations and Maintenance: NCES Operation and Maintenance consists of sustaining the four NCES product lines upon full operational capability, PMO acquisition support, general management and operating expenses, mission support, and civilian pay.

Product Sustainment

Sustainment of the four product lines will commence once the program has successfully achieved a Milestone C decision and has satisfactorily completed the Initial Operational Test & Evaluation (IOT&E) scheduled for FY2008. Sustainment of the four NCES product

I. Description of Operations Financed (continued): By Mission Area

lines includes production management and hosting facility support, quality assurance, information assurance/system security maintenance, and help desk services. Sustainment of the product lines will be the responsibility of the managed service providers that support NCES capabilities; they will sustain NCES product lines in accordance with Performance Work Statements (PWS)/Service Level Agreements (SLA) that are established between the DISA and the service providers. The NCES product sustainment can be categorized as follows:

1. Production Management support includes all costs that encompass a variety of functions for services and programmatic documentation; beginning with the registration of services, the delivery and check-in of software and documentation, storage, and the building, packaging, reproduction and installation of core enterprise service offerings.

2. Hosting Facility Support (Site Support) costs are required to activate and ensure full mission capability of NCES services deployed at each operational site. Hosting Facility Support costs include system and data base administration, system engineering, managed service support, and to ensure specific security requirements are satisfied at each NCES operational site.

3. Quality Assurance support includes resources required after Full Operational Capability (FOC) for Global System Problem Reports (GSPRs) fixes, software upgrades, and services integration maintenance (e.g., all post FOC software investment required to maintain systems integration).

4. Information Assurance/System Security Maintenance support is required for system security fixes and security system upgrades.

I. Description of Operations Financed (continued): By Mission Area

5. Help Desk Services include 24/7/365 availability support, call management, problem management, documentation and reporting.

PMO Acquisition Support

Program Management Office Acquisition support includes all management oversight, fiscal control, contract management, program support, and strategic operations to include planning and communications, program reporting, and program documentation to include the Economic Analysis (EA), Cost Analysis Requirements Description (CARD), System Engineering Plan (SEP), Program Protection Plan (PPP), Information Assurance Strategy (IAS), Acquisition Program Baseline (APB), Acquisition Strategy (AS), Information Support Plan (ISP), Capability Development Document (CDD), and the Concepts of Operations (CONOPS).

General Management and Administration

General management and administration (GM&A) support includes costs that result from all deliverable training services, devices, accessories, aids, equipment and parts used to facilitate instruction through which personnel will learn to operate and maintain the NCES services, and users will learn to exploit the benefits of the NCES services. The GM&A costs also include travel, supplies, training, and equipment for NCES personnel.

Mission Support and Civilian Pay

Mission support costs are the DISA facility operating costs. Civilian pay includes pay to the engineers, analysts, computer scientists, secretaries, IT specialists that support the NCES program.

I. Description of Operations Financed (continued): By Mission Area

Mission: The DoD is transforming warfighter, business and intelligence information technology (IT) operations. Through the use of shared services and information, the DOD Net-Centric Enterprise Services (NCES) Program will use net-centricity to securely interconnect people, information and capabilities, independent of time or location. NCES will substantially improve planning at multiple echelons, provide ubiquitous access to information and services, significantly shorten decision-making cycles, and improve interoperability.

NCES provides the common infrastructure for DOD net-centric operations. It supports the information environment created by the Global Information Grid (GIG) and provides the architectural foundation for the GIG Core Enterprise Services (CES).

The foundation of the NCES net-centric design is a service-oriented-architecture (SOA). This engineering approach creates CES that are available to the DoD warfighter, business and intelligence programs. Special DoD interest groups, or Communities of Interest (CoIs), also can share these capabilities. Using NCES shared available services, frees program resources to develop added unique requirements.

NCES also supports the following five (5) Defense Information Systems Agency Strategic Goals as stated in the Corporate Strategy Scorecard (V.14):

1. Strategic Goal 1: Transition to a net-centric environment to transform the way DoD shares information by making data continuously available in a trusted environment.

2. Strategic Goal 2: Build and sustain a Global Information Grid (GIG) transport infrastructure that eliminates bandwidth constraints and rapidly surges to meet demands, wherever needed.

I. Description of Operations Financed (continued): By Mission Area

3. Strategic Goal 3: Operate, manage, and defend the GIG to enhance critical warfighting and business capabilities in a net-centric environment.

4. Strategic Goal 4: Transition to DoD enterprise-wide capabilities for communities of interest, e.g., warfighting, business, and intelligence, that exploit the GIG for improved decision-making.

5. Strategic Goal 5: Deliver capabilities, based on established requirements, more effectively, economically and efficiently than we do today.

Net-Centric Enterprise Services (NCES) supports the DISA's Strategic Goals one (1), three (3), and four (4) by enabling Community of Interests (COI's) applications and users the ability to exchange information across the enterprise. The NCES supports the DISA's Strategic goal two (2) by allowing authorized users access to the Global Information Grid (GIG) superhighway. The NCES supports the DISA's Strategic goal five (5) by providing periodic program reviews to allow feedback from its users and stakeholders to understand any issues with NCES in providing its services. This feedback enables NCES to correct any deficiencies and improve its services.

NCES will specifically use funds allocated for O&M to sustain all facets of the program, from the NCES product lines to the personnel support needed to execute and maintain the program. A portion of the funds appropriated for O&M will be paid to the managed service providers who provide NCES capabilities to sustain NCES services. The commercial and government service providers will be responsible for the life cycle requirements to provide the services to NCES and DoD. After the ramp-up, the government providers are responsible for any refresh or modifications to maintain or sustain the service to meet latest DoD specifications and standards. The service provider has the complete

I. Description of Operations Financed (continued): By Mission Area

responsibility to sustain and maintain the service at the DoD specifications and standards for an enterprise service and is expected to plan, program and implement for all licenses, software and hardware along with any refresh or updates to existing configurations. The balance of funds appropriated for O&M will be used for program management office acquisition support, general management and administration support, mission support and civilian pay.

b. Global Information Grid Engineering Services (GIG ES)

This Activity includes the DISA's work in the areas of Chief Technical Officer (CTO) and the Systems Engineering Center (SEC).

The Chief Technical Office supports efforts that will strengthen critical Global Information Grid (GIG) technologies and programs through the establishment of the DISA technology strategies, and through the implementation of those strategies in the DISA programs and services. This engineering and technical expertise will be applied in conducting technical reviews of all solutions, products, and services to determine compliance with overall DISA strategy, and to evaluate soundness of technical approach. This effort will support end-to-end reviews of all solutions, programs, and services to ensure all are consistent with GIG architecture and standards. This project supports definition of various aspects of evolving the GIG, including developing system architecture constructs for the GIG and components, providing engineering guidance for component evolution, including incorporation of new technology from industry. Subtasks are assigned based on need to address specific technical problems, mitigate risks, and take advantage of cross-program synergies. Engineering and technical support of the DISA programs implementing the GIG involves technical research and analysis of state-of-the-art and emerging technologies, security, architectures, and application frameworks. This

I. Description of Operations Financed (continued): By Mission Area

involves the identification and recommendation of innovative engineering techniques, technologies and products that are critical to the DISA in its role of instantiating the GIG architecture; the support of information exchanges with the Services, OSD, the Combatant Commanders, and the Joint Staff to identify opportunities, issues, and solutions to improve the DISA products; and facilitation and harmonization of cross-corporate programs relative to the DISA programs and the GIG.

The Systems Engineering Center (SEC) provides architecture, systems engineering and end-to-end analytical functions for the DISA and its customers, enabling integrated capabilities to fulfill warfighter mission requirements. Specifically, SEC performs a broad spectrum of activities for DOD communications planning and investment strategy, to include: application assessments; contingency planning; network capacity planning and diagnostics; lifecycle IT standards engineering activities as the DoD's Executive Agent for IT Standards; and systems-level modeling and simulation. SEC develops across-theater information awareness for Combatant Command through application solutions for integrated networks, to include DOD's missions in Iraq and Afghanistan and the Defense Information Systems Network (DISN), by:

1) Supporting the development and implementation of GIG Enterprise-Wide (EW) Systems Engineering (SE) processes essential to evolving the GIG in a manner that enables interoperability and end-to-end performance for critical GIG programs that are consistent with internal and external components;
2) Developing a standardized DISA systems engineering and integration process to improve systems integration across the DISA for all DISA-developed communication systems and services;
3) Developing, maintaining, and supporting the identification of all individual IT commercial, military (MILSTD), international (NATO) standards and net-centric standards profiles under the Defense Information Technology Standards Registry

I. Description of Operations Financed (continued): By Mission Area

(DISR) process to ensure that such standards are relevant to the evolving Net Ready Key Performance Parameters; and

4) Providing the underlying modeling and simulation and analytical support for end-to-end DISA and DOD systems engineering and assessment.

These SEC operations are to provide DOD decision makers – from the OSD level to the warfighter – with services and a suite of tools capable of identifying key points of impact on DOD command and control information systems and recommending tradeoffs within the GIG configuration with regard to prioritized performance, availability, and security.

With the existing funding, SEC anticipated accomplishments for the Transition to Net-Centric Environment are:

1) Develop, implement and continuously improve on Net-Centric Systems Engineering (SE) processes, enable information sharing and assessing the quality of posted SE results in a shared space for multi-center review, essential to the DISA transition,
2) Stand up a new DISA Strategic Technology Roadmap (DSTR) process outlining a three-tier approach to identify, characterize, and provide guidance on strategic technologies resulting in a standard application approach across the DISA programs. DSTR establishes a venue for joint efforts in investigating emerging technologies that are critical to developing a Net-Centric environment.
3) Identify and develop the Net-Centric standards for GIG Transport, and Enterprise Services, through research and participation in a wide range of industry standards developmental forums and government technical bodies.
4) Provide technical standards direct support to the DISA PEOs development and post-demonstration periods to capture and promulgate Net-Centric standards profiles for DOD-wide use.

I. Description of Operations Financed (continued): By Mission Area

5) Assess Net-Centric Certification under JCIDS requirements to reach a level of maturity in FY08 whereby analysis support tools will be fully integrated and capable of offering labor savings to DOD systems developers in meeting NR-KPP criteria and to capture the state of interoperability of systems in a joint/combined/coalition Net-Centric environment.
6) Analyze and promulgate DISR Net-Centric standards profiles to reach a level of capability in FY08 to support system developers by providing leading-edge Net-Centric information technology standards.
7) Effect messaging standards transition to Net-Centric environment, to include tactical data links, message text formats, and variable message formats, and undergo NetCentric service transition and IP convergence
8) Develop the GIG technical baseline, an E2E Architecture for the GIG, develop an enterprise wide documentation framework for requirements traceability and completeness, the GIG EW roadmap and NCID implementation and compliance enabling interoperation of GIG components that will result in E2E capabilities enabling net-centric operations for the warfighter.
9) Create NCES increment 1 models, based on earlier models developed during the NCES Technology Development Phase. The increment 1 models are used in the development of the NCES System Engineering Plan (SEP) that will support the translation of system capability needs into an effective, suitable product that is sustainable at an affordable cost. This program will provide DOD decision makers with the means to identify the impact of NCES services prior to a conflict or war.

c. Defense Collaboration Tool Suite (DCTS) This project migrated to NCES in FY 2007.

d.

I. Description of Operations Financed (continued): By Mission Area

Advanced Information Technology Services (AITS)

The mission of AITS is to expedite the fielding of mature products into those operational information systems that support the Combatant Commands and our nation's warfighters. The primary mechanism for the transition of the technology is the Advanced Concept Technology Demonstrations (ACTDs). The ACTDs were initiated to allow for the early and inexpensive evaluation of mature or maturing advanced technology to solve important military problems. If an ACTD is successful and proves its military utility, the capability may then transition to a full-blown acquisition program. The warfighter evaluates the technology to determine its military utility before commitments are made for formal acquisition. Products, resulting from AITS ACTDs, may be put under the DISA, or they may be given to a Military Service, DOD Agency, or Combatant Command (COCOM).

In addition, the AITS: a) engineers and reinforces components for leave behind ((US only) after the Military Utility Assessment (MUA) proves that a particular capability is useful and needs to be fielded) and integration into the Global Information Grid (GIG), b) augments transitioning products with improved security, scalability, and Net-Centric Enterprise Services (NCES) compliance; and c) provides advanced, hardened capabilities--Leading Edge Services (LES). LES is a network infrastructure, pilot capability until system of record can provide and deploy the capability, and value added services that include information processing, storage and retrieval; communications (voice, data, video, multimedia); security technology and application in command and control, intelligence, and combat support for the worldwide DoD communities; and information sharing between the US and its coalition partners. ACTD capabilities will be built upon and contribute to Network Centric Enterprises Services (NCES) as they evolve. As components mature in an ACTD, some of its outputs will be network services.

I. Description of Operations Financed (continued): By Mission Area

e. Coalition Warrior Interoperability Demonstration (CWID)

CWID is the Chairman of the Joint Chiefs of Staff's (Chairman's) annual event that enables the US combatant commands, national civil authorities and the international community to investigate command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) solutions that focus on relevant and timely objectives for enhancing coalition interoperability and exploring new partnerships. This event is conducted in a simulated operational environment to provide context for warfighter and national civil authorities' validation of those solutions. Inclusions of national and regional interoperability objectives that augment CWID objectives is encouraged, but remain subordinate to the core objectives and are the responsibility of the sponsor.

(1) Trials are the activities used to address the coalition and interagency interoperability objectives selected each year. Trials strive to address warfighter requirements and interoperability deficiencies. Ideally, they will benchmark successes that can immediately support and enhance operations requiring US, multinational or interagency cooperation. The selection of trials is dependent upon the annual overarching objectives, the host combatant command's priorities, combatant commanders, Services and agencies' (C/S/A's) desire to partner in a proposed trial, interagency participation, the requirements of invited coalition participants and the trial's ability to meet criteria published in the CWID Federal Business Opportunities (FBO) announcement.

(2) The operational environment (simulated) is created by the host combatant command and provides the context for warfighter validation of the proposed interoperability solutions. In general, this consists of a US-led coalition operation with a multinational task force (MTF) staff conducting simulated coalition operations at the combatant command, component and force execution echelons or equivalent interagency level. The

I. Description of Operations Financed (continued): By Mission Area

environment may include elements of homeland security missions. Homeland Defense and Military Assistance to Civil Authorities pose challenges similar to those that multinational military coalitions must address during operations. Interoperability between communication systems is essential. C4 responsibilities may cross multiple intergovernmental boundaries. The CWID provides a forum for exploring solutions to these challenges.

(3) The CWID requires a coalition information environment that will consist of one or more coalition information domains. This environment will interconnect all coalition participants using the CWID Coalition-Wide Area Network (CWAN), a multinational secure network. This network will promote and enable information exchange capabilities among the multiple coalition information domains required to support all participants. CWID will be conducted as a US-sponsored initiative within the Combined Federated Battle Laboratories Network (CFBLNet). The CWID CWAN will utilize the CFBLNet as the permanent baseline for network connectivity. The CWID event may be the culmination of a series of interoperability initiatives conducted over the CFBLNet. The capability to connect this network to national networks, incorporate a variety of coalition participants and promote agile, information exchanges support information superiority, the overall Net-Centric warfare approach and steps toward the implementation of the Global Information Grid (GIG).

f. Information Dissemination Management (IDM) This project migrated to Net Centric Enterprise Services(NCES) effective in FY 2007.

2. Eliminate Bandwidth Constraints: The DISA balanced risks in this area with the new subscription based cost recovery and with offsets in other mission lines by assuming greater institutional risk and reducing key cross-cutting modeling and simulation

I. Description of Operations Financed (continued): By Mission Area

capabilities and limiting growth in standards activities, and (2) limiting the DISA commitments to fund Advanced Concept Technical Demonstrations (ACTDs). Included in this Mission area are:

Mission Area Component ($ in Thousands)	FY 2006 Actuals	FY 2007	FY 2008	FY 2009
a. DoD Teleport Program	16,313	7,068	8,986	8,137
b. Defense Spectrum Organization	27,336	51,066	29,553	32,613
c. Defense Information Systems Network Enterprise Activities	238,256	87,116	89,297	93,026
d. Defense Information Systems Network Subscription	17,375	14,530	16,359	15,279
Eliminate Bandwidth Constraints Total	**299,280**	**159,780**	**144,195**	**149,055**

a. DOD Teleport

The Teleport investment is driven by requirements validated by the Joint Chiefs of Staff and is linked with Defense Information Systems Agency (DISA's) core strategic goal to transition to a net-centric environment to transform the way Department of Defense (DoD) shares information by making data continuously available in a trusted environment. The Teleport system and its capabilities support the Agency's transformational initiatives/goals and the President's Management Agenda by enabling effective communications for the warfighter by early implementation of net-centric capability; enhancing the capability and survivability of space systems and supporting infrastructure; and continuing to develop a joint interoperable Networks and Information

I. Description of Operations Financed (continued): By Mission Area

Integration (NII) architecture. Teleport will provide seamless access to the Defense Information System Network (DISN) and Global Information Grid (GIG), which supports the Department of Defense (DoD)/Joint Staff/DISA goals associated with Command, Control, Communications, Computers and Intelligence (C4I) for the Warrior, and Joint Vision 2020, by providing a global, secured interoperable information transport infrastructure.

Teleport is being deployed incrementally in a multi-Generational FY01-FY12 program. Generation One will field capabilities for four Initial Operational Capabilities (IOC) events. IOC 1 implemented C, X, and Ku band Satellite Earth Terminals and associated baseband equipment at six sites to allow for a deployed warfighter anywhere between certain latitudes to be able to communicate with two Teleport sites. IOC 2 implemented Ultra High Frequency (UHF) Satellite Earth Terminals and associated baseband equipment at four sites. IOC 3 will implement additional C, Ku, UHF, and protected communications (Extremely High Frequency (EHF)) Satellite Earth Terminals and associated baseband equipment at six sites. This will allow the deployed warfighter access to three Teleports from any location (between certain latitudes). IOC 4 will complete the Generation One build-out by integrating military Ka SATCOM capabilities into five Teleport locations. Generation One, IOC 1 reached completion in March 2004. IOC 2 completed in November 2006. IOC 3 will be completed by FY 2007. Generation Two will provide Ka band capacity increases at six sites; it will provide IP capability at six sites; and it will provide Ka band SATCOM terminals at six sites.

The DoD Teleport Program is a Major Automated Information System (MAIS) ACAT-1AM program with the Assistant Secretary of Defense for Networks Information Integration (ASD (NII)) serving as the Milestone Decision Authority (MDA). ASD (NII) Designation Memorandum dated 05 May 2000 identifies the Defense Information Systems Agency (DISA) as the Executive Agent (EA) for the DoD Teleport Program. The system will satisfy Joint

I. Description of Operations Financed (continued): By Mission Area

Requirements Oversight Council (JROC) validated operational requirements. The Teleport Program Office (TPO) received Milestone C Authority to start procurement on 15 April 2002 for Generation One.

The DoD Teleport is a Satellite Communications (SATCOM) gateway that links the deployed warfighter to the sustaining base. It provides high-throughput, multi-band, and multi-media telecommunications services for deployed forces of all Services, whether operating independently or as part of a Combined Task Force (CTF) or Joint Task Force (JTF), during operations and exercises. The DoD Teleport provides centralized integration capabilities, contingency capacity, and the necessary interfaces to access the DISN in a seamless, interoperable and economical manner. DoD Teleport is an upgrade of satellite telecommunication capabilities at selected Standardized Tactical Entry Point (STEP) sites. This upgrade represents a ten-fold increase to the throughput and functional capabilities of those sites. The Teleport system will provide deployed forces with interfaces for multi-band and multimedia connectivity from deployed locations to online DISN Service Delivery Nodes (SDN) and GIG information sources and support. The system will greatly improve the interoperability between multiple SATCOM systems and deployed warfighters.

The O & M funding will be used to provide program management support to the DOD Teleport Program to include salaries, office supplies, equipment, and travel of the PM staff.

The STEP is a DoD Satellite Communications (SATCOM) gateway that links the deployed warfighter to the DISN sustaining base. It provides very high-throughput and multi-media telecommunications services for deployed forces of all Services, whether operating independently or as part of a Combined Task Force (CTF) or Combined Joint Task Force (CJTF), during operations and exercises. The STEP is the lead in providing centralized

I. Description of Operations Financed (continued): By Mission Area

integration capabilities, contingency capacity, and the necessary interfaces to access the DISN in a seamless, interoperable, and economical manner. STEP continues to upgrade satellite telecommunication capabilities at all sites, in conjunction with the DoD Teleport system. Approximately 50% of the DISN services and equipment have been procured, installed, and activated at those joint STEP/Teleport facilities that have been provided by the STEP program, with STEP continuing to make significant upgrades as current and future operational requirements emerge and technology refreshment dictates.

STEP will introduce Internet Protocol (IP) Net-Centric communications to the sites in conjunction with the DoD Teleport program. Net-Centric communications use Internet Protocol for enhanced network interoperability and enable dynamic satellite bandwidth allocation to reduce satellite lease costs and increase overall performance. Extensions from the GIG-Bandwidth Expansion (BE) for global, net-centric capability are already in place at Fort Belvoir, with future integration and simplification of DISN services on-site for extension to the tactical warfighter.

b. Defense Spectrum Organization

DISA merged the Joint Spectrum Center and the Defense Spectrum Office in May 2006 to form the Defense Spectrum Organization (DSO). This realignment reflects the DOD’s ongoing effort to transform spectrum management to meet any future concepts and equipment and to address the President's Spectrum Policy Reform Initiative, which is developing spectrum policies and procedures for the 21st century. The DSO’s mission is to provide integrated strategies, policies, processes, and practices to achieve global spectrum access for national security obligations. The DSO assists the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))with: improving electromagnetic (EM) spectrum management and electromagnetic environmental effects (E3) business processes;

I. Description of Operations Financed (continued): By Mission Area

enhancing the current warfighter spectrum management capabilities to allow for Combatant Command (COCOM) contingency planning; updating spectrum supportability roles and responsibilities throughout the spectrum management community; enhancing acquisition and requirements processes to assure spectrum access; improving future warfighter EM spectrum utilization through technological innovation by researching, studying, and steering the direction of emerging technology advances; promoting EM spectrum and E3 awareness and education through outreach programs that ensure awareness of spectrum-related developments; advocating and defending DOD's EM spectrum needs in national and international EM spectrum forums by developing and executing realistic allocation/reallocation strategies; proactively preparing for the World Radiocommunication Conference 2007; and integrating enabling technology issues in national and international policy development and execution. The key outcome of these initiatives will be the introduction of technological advances into the DOD acquisition cycle allowing for greater warfighter capabilities.

c. Defense Information Systems Network (DISN) - Enterprise

Defense Information System Network (DISN) is DoD's consolidated worldwide telecommunications infrastructure that provides end-to-end information transport for DoD operations, providing the warfighters and the Combatant Commanders (COCOMs) with a robust Command, Control, Communications, Computers and Intelligence (C4I) information long-haul transport infrastructure. The DISN goal remains to span the terrestrial and space strategic domains seamlessly, as well as the tactical domain, to provide the interoperable telecommunications connectivity and value-added services required to plan, implement, and support any operational missions, anytime, and anywhere pushing DISN services to the edge of the communications network. The vision of “power to the edge” is the availability of a “ubiquitous, secure, robust, trusted, protected, and routinely used

I. Description of Operations Financed (continued): By Mission Area

wide-bandwidth that is populated with the information and information services that our forces need."

As a Mixed Life-Cycle Program, the DISN has two major focus areas, Sustainment and Development/Modernization/ Enhancement (DME), with 90+% of the total funding supporting sustainment. The six DISN Lines of Business are DMS, JWICS, Transport Services, Internet Protocol (IP) Services, Real-Time Services, and System Support Services. Transport Services provides a robust worldwide capability of day-to-day voice, video, data and message transmission. With GIG-CS's integration into the DISN Core, Transport continues to accommodate growth in demand with the installation of the OCONUS systems, as well as expanding the CONUS backbone access transmission capabilities. Internet Protocol (IP) Services provides secure internet protocol router network (SIPRNET) as well as non-classified internet protocol router network (NIPRNET) capabilities. It, in conjunction with the Real-Time Services LOB, will address the movement of voice, secure voice, and video service to an IP-based environment. Real-Time Services provides day-to-day commercially competitive voice services plus unique secure military requirements. Video Services provides both routine and classified day-to-day video teleconference. System Support Services contains the elements of network management, provisioning, and customer support services.

The FY 2008 and FY 2009 O&M funding identified will sustain the legacy assets of the DISN through the GIG-CS transition and into the follow-on transformation period associated with the IP convergence effort. The funding is concentrated within three areas, the first (Object Class 23.3) being the purchase of telecommunication services that are an integral part of the DISN infrastructure and not covered under the portion of DISN funded by the Defense Working Capital Fund (DWCF). This includes leases for commercial satellite communications capabilities supporting specific DoD mission areas such as

I. Description of Operations Financed (continued): By Mission Area

Kosovo. The second major expense area (Object Class 25.7) is that of contractor operational support and maintenance activities, again associated primarily with satellite communications, particularly those contracts for the operation of the Defense Satellite Communications System (DSCS) Operational Control System (DOCS), the maintenance of the DOCS supporting ground controller equipment, the DSCS Technical Assistance support contract, the SATCOM Engineering Laboratory, and the Enhanced Pentagon Capability (EPC). Also included in this area are the non-recurring transition costs for DISN optimization and for expiring circuit and bandwidth services contracts. Finally, varied system equipment maintenance acquisitions are expensed within these lines under Object Class 31.3.

d. Defense Information Systems Network (DISN) - Subscription

Enterprise Activities and Subscription Payments is the DoD's consolidated worldwide telecommunications infrastructure that provides end-to-end information transport for DoD operations, providing the warfighters and the Combatant Commanders with a robust Command, Control, Communications, Computers and Intelligence (C4I) information transport infrastructure. The DISN continues to evolve to meet DoD requirements including Mobile Satellite Services (MSS), DISN-Global Broadcast Services Integration (GBS), National Command Authority (NCA) Conferencing Enhancement Project (NCEP) and the GIG-CS, each has added specific activities/requirements. The DISN goal is to span the tactical, terrestrial and space strategic domains seamlessly, to provide the interoperable telecommunications connectivity and value-added services required to plan, implement, and support any operational mission. Driven by both evolving technology, and rapidly increasing customer requirements, the DISN is undergoing a transformation process in two forms: first, technological transformation-driving initiatives such as GIG-CS and the DISN Next Generation (DISN NG) replacement acquisition contracts and, second, the

I. Description of Operations Financed (continued): By Mission Area

business transformation process being implemented through the DoD Enterprise Communications assessments. These initiatives share a common theme – to provide DISN services to the "edge". The vision of "power to the edge" is the availability of a ubiquitous, secure, robust, trusted, protected, and routinely used wide-bandwidth that is populated with the information and information services that our forces need. One of the keys to achieving "power to the edge" is the availability of the ubiquitous IP environment. A primary mission of the DISN, in coordination with Service and CoCOM initiatives, is to provide that environment along with a unique set of interoperable real-time services (e.g., secure/non-secure voice, video-teleconferencing) through the evolution of the Internet Protocol (IP) into a converged IP Environment that, from a warfighters' perspective, is a single physical and logical interface for IP-based services regardless of applications type or classification/access level and provides the levels of performance and availability appropriate for each mission.

The key elements of a ten-year evolutionary timeline are, first, the expansion of the secured core to the edge of the IP network, providing the ubiquitous IP network needed to support net-centric warfare, and second, the use of Net-Centric Enterprise Services (NCES) to achieve IP-convergence in the user interface and applications services. The resulting program requires the maintenance of the current operational baseline services while integrating and transitioning to service those newer offerings such as the GIG-CS and the DISN NG. This resulting breakout consists of the legacy DISN environment through FY 2007 with the integration of GIG-CS, the replacement services for the current DISN associated with the DISN NG, and the optimization of the DISN topology; the transformational vision for the post-GIG-CS and DISN NG transition period from FY 2008 through FY 2011 when the secure IP transport core is expanded further toward the edge and NCES services begin to appear as a basic offering of the DISN service infrastructure; and the end state of FY 2015 when High Assurance Internet Protocol Encryptor (HAIPE)

I. Description of Operations Financed (continued): By Mission Area

implementation has progressed to the information/applications level, the secured core has been extended into the base-level infrastructure, and DISN services have fully exploited the convergence enablers from the NCES program.

The O&M funding sustains the legacy assets of the DISN through the GIG-CS transition and into the follow-on transformation period associated with the IP convergence effort. The funding is concentrated within three areas, the first being the purchase of telecommunication services that are an integral part of the DISN infrastructure and not covered under the portion of DISN funded by the Defense Working Capital Fund (DWCF). This includes leases for commercial satellite communications capabilities supporting specific DoD mission areas such as Kosovo. The second major expense area is that of contractor operational support and maintenance activities, again associated primarily with satellite communications, particularly those contracts for the operation of the Defense Satellite Communications System (DSCS) Operational Control System (DOCS), the maintenance of the DOCS supporting ground controller equipment, the DSCS Technical Assistance support contract, and the SATCOM Engineering Laboratory. Critical contractor operational support work associated with the network management, customer-provisioning support, and network database management is contained within this second expense area. Finally, varied system equipment maintenance acquisitions are supported.

The DoD Enterprise assessments developed a new Price and Governance Process for DISN. The major change between FY 2006 and FY 2007 funding reflects next phase of implementation of the new DISN governance process that involved the transfer of direct DISN funding in the DISA to Services and Defense Agency customers supporting the restructured customer billing concept. The preponderance of telecommunications operations of the DISN are supported through the Defense Working Capital Fund billing and rate processes. FY 2007 funding provides the DISA appropriated activities with the

I. Description of Operations Financed (continued): By Mission Area

resources for the five sites based on direction from the DoD rate board, and support to the SATCOM engineering activities, GIG contract support providing for utilization of the GIG-CS expanded capabilities as directed by DoD acquisition requirements.

3. GIG Network Operations and Defense: Transition demands the continued evolution of GIG in order to provide continuous flow of information from the highest strategic levels to the lowest echelon on the joint battlefield and among the nodes of the net-centric force. However, relying on net-centric capabilities increases operational vulnerabilities unless the information infrastructure can be reliably protected and managed. Network Operations (NetOps) is the operational construct that the Commander, USSTRATCOM, will use to operate and defend the GIG. The Joint Concept of Operations (CONOPS) for GIG NetOps, issued May 2004, defines the DISA's roles and responsibilities associated with the NetOps operational hierarchy and the capabilities needed to implement NetOps with the emerging operational hierarchy.

In addition to the NetOps program, the Operate and Defend the GIG mission area includes the Information Systems Security Program, the ISSP. This Information Assurance program reflects significant increases in FY 2007 and FY 2009 because of the Secretary of Defense's decision to support expanded Computer Emergency Reponses Teams (CERT) requirements and added SIPRNET protections and to add emphasis on Insider Threat activities to improve computer network defense. Based on reduced costs for information security licenses and reduced costs of other security products, funds were realigned from the Procurement, Defense Wide account to the O&M, DW consistent with the Expense Investment criteria ($250K threshold). In addition, this mission area contains the Pacific and Europe Field commands and field offices co-located with the 9 CoCOMs; and the Joint Staff Support Center (JSSC).

I. Description of Operations Financed (continued): By Mission Area

Mission Area Component ($ in Thousands)	FY 2006 Actuals	FY 2007	FY 2008	FY 2009
a. Network Operations	14,471	11,767	11,624	17,941
b. Info Systems Security Program/Info Assurance/PKI	227,996	247,435	251,733	319,579
c. Field Commands and Field Offices	54,821	47,923	49,255	50,297
d. Joint Staff Support Center	5,211	5,855	23,395	24,391
e. GiG Combat Support Directorate				
GIG Network Operations and Defense Total	**302,499**	**312,980**	**336,007**	**412,208**

a. Network Operations (NetOps)

System integration support is purchased to:

- Integrate, customize, and implement Commercial-Off-The-Shelf (COTS) hardware and software, hardware and software license maintenance, and technical support for four operational sites.

- Operate, sustain, and secure Defense Information Systems Agency’s Network Operations (NetOps) Common Operational Picture (DISA NETCOP) systems at all fielded sites.

- Complete Engineer/integrate Spiral 1 requirement tasks; add functional capabilities; integrate the DISA management systems.

- Spiral development, providing enhanced capabilities of system baseline, as well as broadening the scope of the system to provide Global Information Grid (GIG) NetOps

I. Description of Operations Financed (continued): By Mission Area

situational awareness by integrating more NetOps data sources from COCOMs, Services, and Agencies.

b. Information Systems Security Program (ISSP)/Information Assurance (IA)

The DISA Information Systems Security Program (ISSP) has refocused its Information Assurance (IA) efforts by taking a net-centric approach to addressing the DoD's security demands on an enterprise-wide scale. Moving toward a Common Services and shared information model will require our networks to be more transparent and allow users to have seamless access to everything they need to focus on their mission rather than Information Technology (IT) administration. This approach will also require some major adjustments to how IA will be integrated into this new architecture as we focus on designing and deploying proactive protections, deploying attack detection, and on performing IA operations to ensure that adequate security is provided for information that is collected, processed, transmitted, and disseminated on the Global Information Grid (GIG). To rapidly achieve this new vision for defending the GIG, the DISA will: Identify anomalies facing our networks, codify our implementation strategy, align the program with priorities, and evolve to serve as a component of the larger Network Operations (NETOPS) solution.

The ISSP will purchase test and prototype equipment, operate and maintain laboratory and operational equipment, and obtain technical and programmatic consulting services to identify and improve programmatic and technical processes. To support the following goals the DISA is moving towards a model focusing on providing net-centric capabilities on an enterprise-wide scale. To achieve this capability the ISSP will focus its efforts on protecting our vital information, defending our systems and networks, and providing our customers with the ability to maintain information superiority in all environments.

I. Description of Operations Financed (continued): By Mission Area

DISA PROTECTS INFORMATION by creating an environment to safeguard data as it is being created, used, modified, stored, moved, and destroyed, on the communication networks, within the enclave, at the enclave boundary, at the client, and within the computing environment to ensure that all information has a level of trust commensurate with mission needs. The DISA accomplishes this goal by:

- Providing the DoD enterprise-wide antivirus tools to prevent, detect, and eradicate viruses and worms that introduce vulnerabilities negatively impacting the security of the infrastructure.
- Providing enterprise-wide client/server digital certificate licenses which support the issuance of up to 12 million public key certificates.
- Integrating both role and policy based attributes, evolving, operating, and sustaining the Joint Enterprise-wide Directory Services (JEDS) and Global Directory Services (GDS) which allow sharing persistent and reliable identities across the DoD Enterprise.
- Operating and maintaining the Enterprise-wide Cross Domain Service (CDS) which will be expanded to support additional customers, preparing to implement and sustain the XML CDS capability being developed by NSA, and developing a strategy for transitioning the service to the Defense Working Capital Fund (DCWF).
- Developing a Wireless Mapping System and providing mobile and wireless security, engineering, networking, and architecture support and the Secure Mobile Environment Personal Electronic Device service for the enterprise.
- Designing and implementing an initial Authentication and Privilege Management capability that will enable authorization decisions built upon access control methodologies to ensure that any data existing within the enterprise about a user, a situation, or a transaction is available to enable accurate authorization decisions.

I. Description of Operations Financed (continued): By Mission Area

DISA DEFENDS SYSTEMS AND NETWORKS to ensure that no access is uncontrolled and all systems and networks are capable of self-defense by "building in" technologies that recognize, react, and respond to threats, vulnerabilities, and deficiencies. To develop and enforce Computer Network Defense (CND) policies across the enterprise for the purpose of achieving an optimal readiness posture against the outsider "nation state" attacker as well as the threat posed by the insider, the DISA requires sophisticated hardware and software systems to provide technical assistance, vulnerability analysis, and adjudication guidance for network administrators and security officials who work to ensure that all information systems that traverse a DoD enclave boundary are secure. The DISA's efforts under this goal encompass:

- (New) Developing and deploying automated network access controls for the SIPRNet to prevent inadvertent and/or malicious connection of unknown or improperly configured devices to classified DOD networks.
- (New) Providing a robust set of enterprise-wide intrusion prevention and content filtering tools to enhance an existing capability at the boundary between the NIPRNet and Internet that observe, detect, and react to attacks against the Internet Protocol (IP) based infrastructure and/or attached customers.
- Performing robust Certification & Accreditation (C&A) services including penetration testing onsite security reviews, risk assessments, and assistance in the resolution of accreditation issues.
- (New) Expanding existing C&A activities to converge to a common enterprise-wide tool to provide automated support of the new DOD C&A process, ensuring consistency and high quality while reducing time via document management, paperwork reduction, and standardization.
- Sustaining and expanding to the enterprise existing subnets called Demilitarized Zones (DMZs) that sit between trusted internal networks and untrusted external networks and

I. Description of Operations Financed (continued): By Mission Area

protect the DoD infrastructure while simultaneously improving the ability for authorized users to access shared data while keeping them away from unshared data capabilities.

- (New) Expanding NIPRNet DMZs to provide scalable infrastructure to allow full migration of all outward facing applications.
- (New) Expanding SIPRNet DMZs to force all traffic from/to external networks through the DMZs to establish a more definite SIPRNet perimeter.

- Sustaining the Secure Configuration Compliance Validation Initiative (SCCVI) and Secure Compliance Remediation Initiative (SCRI) enterprise-wide tools that automatically identify configuration vulnerabilities and automatically correct the reported vulnerabilities.
- Conducting reviews to ensure compliance with security policies and assessing the risks of protecting the SIPRNet and NIPRNet.
- Providing specialized perimeter defense engineering and support to assist the CC/S/A's in the deployment of firewalls at enclaves and non-DoD access points and connections.
- Sustaining and operating a centralized repository for DoD users to register ports and protocols used in their Automated Information Systems (AISs) to enable interoperability while simultaneously restricting unauthorized access to those systems.
- Providing technical support for deploying robust tools to over 1500 sites across the DoD enterprise-wide to analyze, detect and respond to an insider threat to information and information systems.
- Initiating the development of enterprise tools for mapping threats and vulnerabilities to risks to provide customers with a better understanding of how susceptible their environments are to attack.
- Identifying and providing across the enterprise configuration standards, automated assessment tools, and security guidance for systems, networks, and applications.

I. Description of Operations Financed (continued): By Mission Area

- Providing on-site IA technical expertise at Combatant Command sites to analyze and identify critical security deficiencies, implement system improvements, support the deployment of IA enterprise tools, and analyze the effectiveness of IA programs.
- Providing certification support and developing accreditation recommendations for the Designated Approving Authorities (DAA) at the DISA enclaves and installed applications.
- Sustaining the DoD enterprise Vulnerability Management System (VMS) used to track vulnerabilities in support of: the IA Vulnerability Management (IAVM) program; the Joint Task Force–Global Network Operation (JTF-GNO) task order acknowledgement and compliance process; the IA Readiness Review (IARR) process; the FISMA process; and the Computer Network Defense Service Provider (CNDSP) C&A program.
- Providing an enterprise-wide tool to configure operating systems by automatically setting permissions, making registry changes, installing patches, and disabling unneeded services.
- Operating and maintaining the enterprise-wide SIPRNet & NIPRNet patch management system used to distribute and install vendor patches, tools and updates.
- Sustaining the enterprise-wide host information database that translates names into IP addresses.
- Deploying and maintaining militarized versions of Intrusion Detection Systems (IDS) that identify unauthorized traffic and access intrusions at the enclave, network, and host computer network levels of the GIG; and characterize the type of attack to enable circumvention at the network site by blocking the activity at the router or firewall.
- Providing an enterprise-wide risk management and accountability process and central repository for connecting enclaves to the SIPRNet to verify the connection belongs to a valid DoD user, the required accreditation processes are complete, and as a source for information that would be needed to disconnect DoD from the Internet.

I. Description of Operations Financed (continued): By Mission Area

- Providing engineering services and support to secure current and planned DISN network infrastructure, evaluation of policy on IA architecture, and development of implementation strategies for securing the GIG.
- Sustaining the robust network foundation needed for secure, world-wide, net-centric operations by evaluating cutting-edge technologies and recommending deployment solutions for improving the security posture for the management and control of data transferred over the DISN.

DISA Delivers Integrated IA Situational Awareness (SA) and IA Command and Control (C2) by providing decision makers and network operators at all command levels the tools for conducting IA and Computer Network Defense (CND) operations in Net-Centric Warfare (NCW). To support this goal the DISA is:

- Sustaining the operation of enterprise-wide tools for collecting, storing, retrieving and analyzing header flow data and metadata from the border routers on the NIPRNet and the backbone routers on the NIPRNet and SIPRNet.
- Developing and deploying an enterprise-wide security application with a central manager to protect every host or node in the network.
  - (New) Provide full implementation of attack detection and response capabilities via the host based security system.
- Identifying a standard for Tier 3 Security Information Managers (SIMS), supporting a pilot deployment, and establishing a Blanket Purchase Agreement (BPA) to enable enterprise-wide purchases by the services and agencies.
- Providing a capability to share integrated situational awareness data to allow analysts and commanders to collaborate, formulate courses of action, and evaluate resultant impact on local, intermediate, and DoD-wide CND activities and operations.

I. Description of Operations Financed (continued): By Mission Area

- Developing and deploying a tool for capturing and analyzing hacker exploit data to categorize new threats and support the employment of network protection countermeasures.
- Sustaining enterprise-wide Tier I/II SIMs used to reduce and correlate voluminous amounts of data generated by GIG IA/CND sensor systems.
- Providing technical management and assistance, development oversight, and maintenance for a suite of computer incident reporting and tracking databases which allows Computer Emergency Response Team (CERT) analysts across the enterprise to share data and resources to ensure rapid and secure retrieval of information to support decisions.
- Conducting security reviews for the Commandant Commands to analyze the effectiveness of their IA programs and their ability to protect their information resources from attack or compromise.
- Providing an automated capability to monitor and report security policy compliance for critical DoD assets using "behavior" based anomaly detection to trigger alerts based on the presumption that deviations from known behavior are suspicious.
- Developing and deploying enterprise-wide tools to provide the capability to trace cyber attacks to their sources and accurately identify and characterize the attacking activity information warfare capabilities.
- Providing an enterprise-wide capability to collect, analyze, and report significant threats to the GIG.
- Coordinating a constellation of enterprise-wide sensors to look for intrusions and anomalies at the enclave, network and host levels.

DISA TRANSFORMS AND ENABLES IA CAPABILITIES innovatively by discovering emerging technologies, experimentation, and refining the development, delivery and deployment processes to improve cycle time, reduce risk exposure and increase return on investments

I. Description of Operations Financed (continued): By Mission Area

to create a broader awareness, understanding, and knowledge base from which the IA community can grow. The DISA supports this goal by:

- Collaborating with the NSA to deliver a forum for DoD IA community to identify and resolve relevant IA issues, develop strategies, and demonstrate new technologies.
- Providing a robust web-based tool for disseminating IA documents, related links, resources and additional support across the enterprise.

DISA CREATES AN IA EMPOWERED WORKFORCE that is well equipped to support the changing demands of the IA environment by establishing baseline certifications across the enterprise, continuously enhancing IA skills to keep current with technology and threats, providing training for skilled people where needed, and infusing IA awareness and concepts into other disciplines and activities. The DISA's efforts under this goal involve:

- Developing and disseminating standardized Computer Based Training (CBT), Web Based Training (WBT) and video overviews, descriptions and guide products.
- Designing and delivering hands-on IA classroom training to security professionals, system and network administrators, and system users throughout the joint community.
- Providing training products to support the professionalization and certification of the DOD IA workforce.

c. Field Commands and Field Offices

Field Commands and Field Offices resolve in a time-sensitive manner and function as the focal point for all DISA and theater-unique requirements. They maintain a proactive role with other Field Offices/Commands and Combatant Command

I. Description of Operations Financed (continued): By Mission Area

representatives, managing requirements including identification; delivery of the DISA services; theater situational awareness. In addition, the DISA Continental U.S. (CONUS) provisions, exercises centralized management of the DISA's networks and is responsible for the real-time operational direction, monitoring and control of the DISA networks.

d. Joint Staff Support Center

JSSC conducts 24x7 watch/monitor operations in the National Military Command Center (NMCC) for Communications, Command, Control, Computer and Intelligence (C4I) systems, strategic threat operational warning, and local Global Command and Control System (GCCS)-Joint operations maintenance. JSSC provides the Joint Staff (JS) with software-applications support relating to operational capabilities in conventional and nuclear planning and operations. JSSC also provides studio and remote video and audio recordings, electronic graphics, postproduction editing for Defense-wide training, informational, gun camera and battle damage assessment assistance, guidance for video teleconferencing networks and operations. Additionally, JSSC provides Continuity of Operations for C4I capabilities in direct support of the Joint Staff. Funding provides civilian salaries and benefits, contract labor, hardware/software maintenance, training, travel, and equipment lifecycle support. FY 2008-2009 funding has been increased to support the additional Nuclear Planning and Execution System (NPES) contract labor requirement due to the increase in NPES mission requirements. FY 2008 – FY 2013 reflect an internal organizational realignment of funds to support JSSC's local mission and non-GCCS-J C4I support. This was a result of the GCCS-J global operational sustainment migration from JSSC to Computing Services (CS).

I. Description of Operations Financed (continued): By Mission Area

4. Exploit the GIG for Improved Decision Making: This mission area funds key Command and Control activities including the Global Command and Control System-Joint (GCCS-J); the Global Combat Support System (GCSS), National Military Command System (NMCS); Defense Message System (DMS); Common Operating Environment (COE); Joint Command and Control (JC2); Joint Interoperability Test Command (JITC). The GCCS Family of Systems programs to deliver C2 capabilities specified in their respective requirements documents, and plan to transition GCCS to a joint, net-centric C2 capability. The DISA has also realigned resources in GCCS-J to support the migration of the Joint Operation Planning and Execution System global mission from the JSSC to the Defense Enterprise Computing Centers (DECC). The DISA will continue to support key GCCS-J activities to develop and field joint C2 capabilities until a successor set of capabilities is formally approved. Included in this mission area are other programs including JITC support services and Counter Drug Transfer.

e. Mission Area Component ($ in Thousands)	FY 2006 Actuals	FY 2007	FY 2008	FY 2009
a. Global Command and Control System-Joint	92,774	87,678	72,145	84,796
b. Global Combat Support System	15,244	14,623	15,192	17,042
c. National Military Command System	3,420	28,580	5,789	5,893
d. Electronic Commerce	30,646	0	0	0
e. Defense Message System	19,476	18,550	15,140	17,628
f. Common Operating Environment	9,982	14,617	5,889	4,007
g. Testing	28,008	0	0	0
h. Combined Enterprise Regional Information Exchange System	1,914	26,806	25,265	24,715

I. Description of Operations Financed (continued): By Mission Area

i. Net-Enabled Command Capability (CivPay & Shared Services)	3,848	6,216	6,294	6,562
j. Other programs	28,490	15,729	13,824	13,687
Exploit the GIG for Improved Decision Making Total	**233,802**	**212,799**	**159,538**	**174,330**

a. Global Command and Control System-Joint (GCCS-J)

The Global Command and Control System-Joint (GCCS-J) is the Department of Defense joint Command and Control (C2) system of record for achieving full spectrum dominance. GCCS-J is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture of the battle space necessary to conduct joint and multinational operations. It enhances information superiority and supports the operational concepts of full-dimensional protection and precision engagement. GCCS-J provides a robust and seamless C2 capability to the Commander-in-Chief, Secretary of Defense, National Military Command Center, Combatant Commanders, Joint Force Commanders, and Service Component Commanders. Employing the Defense Information Systems Network, GCCS-J offers vital connectivity to the systems the joint warfighter uses to plan, execute, and manage military operations. GCCS-J is a major Information Technology investment and is designated an Acquisition Category IAM Major Automated Information System (MAIS) program. GCCS-J is being implemented in an evolutionary manner through distinct blocks, using spiral development. Each block is self-contained, targets a specific set of Joint Staff validated, prioritized user requirements, and deliver multiple releases of GCCS-J functional capabilities. GCCS-J employs a predominantly open system client/server architecture, which is evolving to a web-based architecture that allows a diverse group of commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) software packages to operate at any GCCS-J location. GCCS-J integrates C2 mission

I. Description of Operations Financed (continued): By Mission Area

applications/capabilities, database, web technology, and office automation tools. It fuses select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information.

GCCS-J is used by all nine combatant commands at sites around the world, supporting joint and coalition operations. This effort provides 24 x 7 global help desk support, via the Joint Operations Support Center (JOSC) and the National Military Command Center. The JOSC is the primary entry point for resolving all operational GCCS-J hardware, software and network issues.

In the Common Operating Environment (COE) memorandum (3 January 2005), the Assistant Secretary of Defense, Network Information Integration (ASD-NII) Office issued guidance to the military departments, services, and defense agencies stating that COE compliance is required for software intended to run on the GCCS-J or the GCCS Family of Systems (FoS). In 2006, the decision was made to move the COE program under the GCCS-J PMO. Beginning in FY2008, GCCS-J will be responsible for the sustainment of the COE. The sustainment of the COE components during this transition is critical until GCCS-J is able to field a non-COE version of the software and provide this same software to the Service-specific C2 systems.

Collaborative Force Analysis, Sustainment, and Transportation System (CFAST): Adaptive Planning (AP) is the DoD's methodology for constructing timely and agile war plans that achieve national security objectives. The Collaborative Force Analysis, Sustainment, and Transportation System (CFAST) is a suite of software tools that provides AP capabilities to include: campaign planning, forecast predictions, information management and rapid execution. As an operational prototype, CFAST will continue to evolve as required to support the Joint Planning and Execution Community (JPEC) and is aimed to reduce the

I. Description of Operations Financed (continued): By Mission Area

deliberate planning timeline from two years to six months. CFAST facilitates the dynamic preparation of campaign plans for rapid expeditionary environments to meet DoD planning doctrine requirements of ongoing operations such as the Global War on Terrorism (GWOT) and future contingencies. The U.S. Pacific Command (USPACOM), U.S. European Command (USEUCOM), Joint Staff, and other Combatant Commands currently utilize CFAST. OSD and Joint Staff use CFAST to model how DoD will respond to current and future conflicts using a variety of current and future forces for all Services as part of their Operational Analysis missions.

b. Global Combat Support System (GCSS)

The Global Combat Support System (Combatant Command/Joint Task Force) (GCSS (CC/JTF)) is an initiative that provides end-to-end visibility of retail and unit level Combat Support (CS) capability up through the National Strategic Level facilitating information interoperability across and between CS and Command and Control (C2) functions. GCSS for the Combatant Command/Joint Task Force commanders (CC/JTF) provides decision makers with fused CS data and C2 information on the same workstation. In conjunction with other Global Information Grid elements including Global Command and Control System-Joint, Defense Information System Network, Defense Message System, Defense Enterprise Computing Centers – Detachments, and Combatant Commands/Service/Agencies information architectures, GCSS (CC/JTF) will provide the information technology (IT) capabilities required to move and sustain joint forces throughout the spectrum of military operations.

Per Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6723.01, within the GCSS Family of Systems (FoS), the DISA is responsible for two main efforts: System Architecture and Engineering for the GCSS FoS, and development, integration, fielding, operation and maintenance of the Global Combat Support System (CC/JTF). GCSS (CC/JTF)

I. Description of Operations Financed (continued): By Mission Area

provides enhanced CS situational awareness to the joint warfighter by integrating CS information into the C2 environment, and facilitating communications between the forward deployed elements and the sustaining bases, ultimately resulting in faster, more efficient decision making by the joint warfighter. GCSS (CC/JTF) significantly increases access to information stored in disparate databases via a single sign on, web Portal application, using a SIPRNet PKI certificate. The GCSS (CC/JTF) provides an infrastructure that allows secure web-access, discrete user account administration, data mediation, and enterprise management features, providing the springboard for delivery of capabilities to meet the vision of the future Net-Centric environment. GCSS (CC/JTF) is postured to accomplish the objective Net Centric Vision by using web-based technology to meet the Focused Logistics tenets of Joint Vision 2020 (JV 2020). The DISA Balanced Scorecard Corporate Strategy "C-4 Transition to DoD enterprise-wide capabilities for COI (e.g., command and control, combat support) that exploit the GIG for improved decision-making" is directly supported by the decision support tools and federated applications delivered by GCSS (CC/JTF).

From FY 2007 through FY 2009, the program is incrementally implementing a service-oriented architecture in a net-centric environment utilizing the NCES core concepts as well as new Enterprise Information Integration (EII), Business Intelligence, Workflow, Knowledge Management, Web Service Management, and Security tools. The architecture includes implementation of a more robust Continuity of Operations Plan (COOP), failover, Enterprise System Management (ESM), and security (e.g., intrusion detection on GCSS strategic servers and next generation guards) processes and tools. This new architecture will enable the program to become fully net-centric and enable accelerated introduction of new data source integration and application development, greater flexibility for the end-user in how they evaluate and view fused data, provides dynamic report capability, enables more rapid exposure of data to communities of interest, and increased security.

I. Description of Operations Financed (continued): By Mission Area

This architecture migration directly supports the DISA Balanced Scorecard Corporate strategy ”C-1 Transition to a net-centric environment to transform the way DOD shares information by making data continuously available in a trusted environment.”

c. National Military Command System (NMCS)

NCMS provides Senior Leaders, National Military Command Centers (NMCC), Executive Travel Fleet, Office of the Secretary of Defense (OSD), Chairman, Joint Chiefs of Staff (CJCS), and the President of the United States support to maintain C2 capabilities, ensure continuous availability of emergency messaging, and maintain situational and operational awareness. The DISA Command Center Engineering, within the Strategic Communications Branch, provides innovative and cost-effective engineering solutions to ensure that the NMCS components and facilities located at the NMCC and NMCC Site R provide the Joint Staff with the necessary emergency messaging, situation awareness, crisis action, and operational capabilities. The goal of this support is to provide overall configuration management and guide the future evolution of the many systems in the NMCS while continuing to meet users’ needs. Projects support the Director’s objective of providing responsive, timely, and accurate information to the warfighter. The program provides concept development, requirements definition and calibration, technical specifications, proofs-of-concept, testing, rapid prototyping, technology insertions, systems engineering and integration and technical assessments. Additionally, support provides informed, decision-making linkage between DoD Executive Leaders and the Combatant Commanders of the Unified and Specified Commands.

From FY 2007 through FY 2009 configuration management of NMCS assets including C2 systems and facilities (including transition planning for relocation of current NMCC/HEMP Facility to new NMCC); technical assessments and engineering support to modernize the

I. Description of Operations Financed (continued): By Mission Area

NMCS via technology insertions and implementation of an Information Resources Management (IRM) infrastructure; migration of NMCS messaging systems to Defense Message System (DMS) architecture; and mirroring of NMCC systems at the Alternate NMCC via the Site R Integration Program. Funding supports NMCS/NCC integration and implementation actions as informed by various OSD, USSTRATCOM, and DISA studies for integrating nuclear command and control systems with Global Strike, Missile Defense, and crisis response command and control systems to enable a robust, responsive, scalable architecture of mobile and fixed nodes underlying future solutions for emerging National command and control requirements. Activities include developing and implementing changes to survivable mobile command centers, terrestrial and SATCOM network topologies, and supported operational capability architectures and roadmaps.

d. Electronic Commerce (eCommerce)

In FY 2005 the Deputy Secretary of Defense established the Business Transformation Agency (BTA) to consolidate all business improvements under the auspices of the Undersecretary of Defense for Acquisition, Technology and Logistics. As a result, the ECommerce program transferred from the DISA to the BTA in FY 2006, with all resource transfers completed in FY 2007.

e. Defense Message System (DMS)

DMS is the Warfighter’s Message System, providing secure, accountable, and reliable messaging and directory service at DoD sites worldwide. The Office of Assistant Secretary of Defense for Networks and Information Integration (OASD/NII) directed development of DMS and mandated DoD’s transition from legacy systems to DMS. DMS

I. Description of Operations Financed (continued): By Mission Area

fulfills Joint Staff validated and prioritized operational requirements for an integrated writer-reader capable, organizational messaging system that is accessible worldwide, (to include tactically deployed military personnel), and interfaces to our Allies, non-DoD agencies, and Defense contractors. The primary focus of DMS is to provide a disciplined interoperable organizational messaging environment that leverages commercial products to the maximum. DMS utilizes Commercial-Off-the-Shelf (COTS) and modified COTS components to provide multi-media messaging and directory capabilities that complement and leverage the Global Information Grid (GIG). DMS capability exceeds that of pure COTS applications. DMS products incorporate state-of-the-art information technologies, including the internationally developed Allied Communications Protocol (ACP) 120 implementation of the Common Security Protocol (CSP), which provides automated access controls for compartments, code words, and caveats. It provides the full range of messaging services to meet organizational and individual messaging needs throughout the DoD. NSA class 4 Public Key Infrastructure (PKI) certificates are used for authentication and access control. DMS will reliably handle information of all classification levels (Unclassified to Top Secret), compartments, and special handling instructions.

The DMS received its Milestone III approval from ASD/C3I in July 2002 and was placed into its sustainment phase (by ASD/NII) in May 2005. During the sustainment phase, system/product modifications and associated integration and testing are focused on commercial evolution, security improvements to meet changing security threats, and minor product usability improvements. A mixed life cycle approach is used to address COTS modifications.

I. Description of Operations Financed (continued): By Mission Area

f. Common Operating Environment (COE)

COE provides the foundation infrastructure to promote and enhance interoperability of command and control systems and related capabilities across the Department of Defense. The COE's Common Operational Picture is used to provide a single view of battlespace situational awareness to commanders at all echelons from tactical to strategic. Funding through FY 2011 will provide basic maintenance support to the GCCS Family of Systems. The COE is nearing the end of its life cycle and is thus in a sustainment mode. In the *Common Operating Environment (COE)* memorandum (3 January 2005), the Assistant Secretary of Defense, Network Information Integration (ASD-NII) Office issued guidance to the military departments, services, and defense agencies stating that COE compliance is required for software intended to run on the Global Command and Control System – Joint (GCCS-J) or the GCCS Family of Systems. Minimum COE compliance requirements will phase out as GCCS-J is retired from the inventory and software applications are migrated to the Joint Command and Control portfolio.

From FY2007-FY 2009, COE will provide basic maintenance support. During the transition to a net-centric environment, COE customer requirements for COE sustainment services, including mission critical operational support, will continue. These requirements include cross-program, inter-service/inter-agency support for resolution of critical engineering issues, information assurance vulnerability analysis (IAVA), and computer incident emergency response. Other services provided by the project office include trouble shooting, integration and testing support, patch releases for critical software failures, information assurance/computer security integration support, software configuration management, and software asset distribution services.

I. Description of Operations Financed (continued): By Mission Area

g. Testing

The Defense Information Systems Agency's Testing efforts fund civilian salary and operating costs associated with the test and evaluation mission. This area focuses on test and evaluation standards, policies, and procedures; testing laboratory infrastructure; technical administrators and personnel; and supplies necessary to test and evaluate information technology programs. Testing provides testing laboratory infrastructure and management including information technology equipment, software and hardware maintenance and licensing, technical support, security, network communications, travel, and training. Testing develops transformational test and evaluation concepts to ensure agile and capability-focused processes for information technology systems and services. This area also provides test and evaluation oversight to ensure consistent application of sound methodologies and quality reporting. Testing develops the DISA's test and evaluation standards, policies, and procedures and monitors the implementation of the standards, policies, and procedures.

h. Combined Enterprise Regional Information Exchange System

The Multinational Information Sharing (MNIS) Program shares operational and intelligence information with multinational partners using three current capabilities of the Combined Enterprise Regional Information Exchange System (CENTRIXS). CENTRIXS supports intelligence and classified operations; information exchange and sharing at the Secret Releasable (REL) level. There are multiple, cryptographically-isolated CENTRIXS enclaves serving various communities of interest (COI) that support multinational efforts to include Operation Enduring Freedom (OEF), Operation Iraqi Freedom (OIF), and the Global War On Terror (GWOT). These networks allow the United States to share information rapidly with coalition partners worldwide in support of local, regional, and global combined

I. Description of Operations Financed (continued): By Mission Area

operations. The CENTRIXS architecture is both network-centric and web-centric, using a combination of readily available commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) solutions to reduce implementation costs while providing a robust, innovative approach to warfighting communications. CENTRIXS services include providing common and consistent situational awareness of the battlefield via Common Operational Picture (COP), Common Intelligence Picture (CIP), Intelligence, Surveillance and Reconnaissance (ISR), information and improved information sharing via secure Voice over Internet Protocol (VoIP) telephony, Web Services, Email with attachments, and other information services supporting coalition operations. To date, CENTRIXS has been employed at five Combatant Commands with connectivity in 78 nations. Funding will add four new sites and support a CENTRIXS Network Control Center (CNCC) for three domains: Global Counter Terrorism Forces (GCTF), Multinational Coalition Forces Iraq (MCFI), and CENTRIXS Four-Eyes (CFE), and, provide network operations (NetOps) situational awareness to the Department of Defense (DoD) and Combatant Commands (COCOMs) concerning the health, security and operation of these networks. In FY 2008 and beyond, funding sustains the CENTRIXS-enhanced footprint and enables continued coalition information sharing in support of the afore-mentioned multinational efforts.

Per guidance provided by the Quadrennial Defense Review (QDR) dated 6 February 2006, the Joint Staff (J6) recommended the expansion of CENTRIXS footprint for a “deeper, wider, richer information exchange environment”. The FY 2008 President’s Budget transfers functional responsibility for MNIS from the Navy to the Defense Information Systems Agency (DISA) to maintain current capabilities and supports an increase in the MNIS mission.

Funding will continue current operational support to CENTRIXS including procurement, logistics, training, and, associated technical/engineering expertise necessary to

I. Description of Operations Financed (continued): By Mission Area

maintain and sustain these systems. Additionally, funds will be used to complete centralization of service hosting and convergence of CENTRIXS and Griffin capabilities into a single capability allowing approved interaction between national Secret domains for the Combined Communications Electronics Board (CCEB) nations, enterprise services for CENTRIXS users, and information sharing between and among CENTRIXS domains using the necessary guarding technologies, policies, and procedures to ensure that the right mission partners can access the right information in a timely fashion.

5. Deliver Capabilities Effectively/Efficiently: This mission area funds the DISA Management Headquarters activities, payments levied to fund the costs that the DISA incurs as a Pentagon and deployment site tenant, as well as the Shared Services Units, the organizational activities required to run an agency and support the major programs and functions in their efforts to deliver capability to the warfighter and other customers.

Funds for the International Cooperative Administrative Support Service (ICASS) are also included. ICASS is a cost sharing system for the administrative support that the U.S. State Department provides to Federal Departments and Agencies, to include the DoD.

DISA's performance metrics concept commits the agency to provide greater transparency, quality, and timeliness of financial information; and to manage all costs to ensure best value for our customers. As a necessary first step towards these goals, the DISA established a methodology for consistently assigning shared costs across programs and activities. These shared costs include, but are not limited to: facilities operations and maintenance costs for the National Capital Region, force protection costs both prior and subsequent to 9-11, DFAS bills, centralized costs of financial information systems, vendor management costs of awarding and administering contracts, operating costs of

I. Description of Operations Financed (continued): By Mission Area

payroll and human resources management systems for civilian and military personnel, centralized training and career development efforts, travel services, disability payments to the Department of Labor, and the operating and investment costs of the DISA's internal LANs, WANs, and IT services. These shared costs also include the pay and benefits of the government staff involved in managing or providing these shared services. In the past, these costs were allocated to the legacy organizations that originally incurred these costs, rather than the consumers of these services.

Implementing this initiative significantly improves the DISA's presentation of the total cost of programs to OSD, OMB, and Congress, and addresses weaknesses identified by GAO and OMB. It will preclude unintended subsidies to Defense Working Capital Fund operations in the agency, addressing concerns in this area expressed by both GAO and Congressional Committees. This initiative redistributes costs across programs and activities in the DISA to identify the total cost of ownership of a program. Most importantly, the implementation of this methodology does not decrease the amount of direct funding available to any program or activity in the agency. However, in the future, as program decisions are made this allocation will identify the increase the support costs incurred by a specific program, those increases will be apparent in changes to the program resources.

Mission Area Component ($ in Thousands)	FY 2006 Actuals	FY 2007	FY 2008	FY 2009
a. Management Headquarters	33,321	37,192	34,126	34,635
b. Pentagon Reservation Maintenance Revolving Fund	13,658	13,278	14,142	14,707
c. Shared Service Units	33,511	27,664	18,284	15,003
Deliver Capabilities Effectively/Efficiently Total	**80,490**	**78,134**	**66,552**	**64,345**

I. Description of Operations Financed (continued): By Mission Area

a. Management Headquarters

Management Headquarters funds provide resources for overseeing, directing, and controlling the DISA activities. The DISA activities include both those funded with appropriated funds and Defense Working Capital Funds (DWCF). The Management Headquarters staff provides the leadership for implementing and responding to the OSD mandate to establish Agency performance goals and track results. The staff provides Agency-wide policy guidance; reviews and evaluates overall program performance; allocates and distributes Agency resources, and conducts mid and long-range planning, programming, and budgeting. Inasmuch as Agency Management deals with planning (both strategic and operational), overseeing, controlling, and directing the DISA activities, Management Headquarters outputs and products primarily consist of policies, guidelines, and procedures in support of information technology (IT) related products and services, such as long haul communications, command and control and combat support systems, computing services, and other warfighter capabilities delivered through the wide variety of major system acquisitions for which the Agency is responsible. The activities include technical and administrative support essential to the operation of the DISA and supportive of Global Net-Centric solutions. Additionally, Management Headquarters accounts for Agency-wide congressionally mandated functions, such as the Equal Employment Opportunity Office and the Inspector General.

Supporting outputs and products include: performance budgets that document the annual outputs and long-term outcomes of the work the DISA performs with the resources it receives; the Agency Balanced Scorecard (BSC) that establishes corporate-level performance metrics and a management framework to help the DISA managers balance investment priorities against risk over time; the DISA Strategic Plan that provides the framework for the DISA organizations to develop their appropriate level goals,

I. Description of Operations Financed (continued): By Mission Area

objectives, and performance measures to ensure the link with overall Agency goals and objectives and unity of purpose; the DISA 500 Day Action Plan that highlights the highest priorities of the DISA's customers to ensure that the DISA provides the Commander in Chief, OSD, the Joint Staff, Combatant Commanders, Services, Agencies, and others with world-class information products and services; and Annual Program Plans and follow-on quarterly Financial Health Assessments that assist DISA leaders in ensuring good stewardship of the resources the DISA receives. The challenges addressed by the Agency senior leaders revolve around the achievement of the DISA's Strategic Goals.

b. Pentagon Reservation Maintenance Revolving Fund (PRMRF)

United States Code, Title 10, Section 2674 established the Pentagon Reservation Maintenance Revolving Fund (PRMRF). This statute authorizes the Secretary of Defense to establish rates and collect charges for space, services, protection, maintenance, construction, repairs, alterations, or facilities provided at the Pentagon Reservation. The relationship is similar to that of landlord and tenant in the private sector. The Washington Headquarters Services (WHS) charges tenants "rent" for the services WHS provides. The Defense Information Systems Agency (DISA) PRMRF costs are included in this activity group.

c. Shared Services Units (SSUs)

SSUs resources are allocated across the products and services contained in the business and mission activities. The model uses four primary cost drivers: (1) number of authorized billets (civilian and military), (2) number of DISANet accounts (civilian, military, and contractor), (3) number of tenants in National Capitol Region facilities

I. Description of Operations Financed (continued): By Mission Area

(civilian, military, and contractor), and (4) amount of dollars in the business and mission projects.

- Chief Financial Executive (CFE) funds the salaries and operating expenses of the CFE to provide financial services support and financial automation support to the Agency and perform requirements of the Chief Financial Officer (CFO) Act and the Government Performance and Results Act as well as the Budget and Performance Integration goal of the President's Management Agenda (PMA). CFE conducts economic analyses, cost estimating and program and organizational assessments. A major challenge is to provide accurate, reliable, and timely financial information to support the DISA's planning, engineering, acquiring and fielding of the Global Net-Centric solutions and operating the GIG. Funds the payments due to the DFAS and contract support in the areas of accounts payable and support (receiving, processing and filing the DISA vendor and intra-government invoices/bills); enhancements to the Defense Financial Management System in support of Agency operations; continuing implementation of the CFO Act to include preparation of the annual, Agency-wide financial statements and implementation of metrics associated with the Balanced Scorecard. FY 2006 funding initiated the business process reengineering and requirements analysis to transition the DISA to the DISA Standard Finance and Accounting Systems (DSFAS); the DoD integrated Financial Management System; as well as the auditing and related activities to implement the Financial Management Improvement Plan requirements. FY 2007 to FY 2009 continues implementation and contractor support for a clean financial audit opinion.

- Component Acquisition Executive (CAE) In August of 2002, the Principal Director of Applications Engineering was designated to perform the DISA's Component Acquisition Executive (CAE) duties as collateral responsibilities to the existing Directorate duties. This organizational structure presented a management challenge since the acquisition

I. Description of Operations Financed (continued): By Mission Area

activities were located throughout the agency with no clear line of authority between the CAE and the Program Managers. The lack of clear accountability and ambiguous line of authority was identified as a structural weakness by the Office of the Secretary of Defense Networks Information Integration (OSD/NII) who recommended clear alignment of responsibility and authority via a short, unambiguous chain of command.

On 1 October 2003, a dedicated Component Acquisition Executive (CAE) was established to focus exclusively on all acquisitions managed by the DISA to include Major Automated Information Systems (MAIS), IT Services, Acquisition Category (ACAT) III programs, projects and services being acquired by the DISA. The purpose of the CAE program activities is to achieve successful implementation of the net-centric vision by providing tailored acquisition policies, procedures, tools, lifecycle oversight, and career management in compliance with statutory and regulatory requirements. As outlined in the May 12, 2003 DoDD 5000.1, the Defense Acquisition System exists to manage the nation's investment in technologies and programs necessary to achieve the National Security Strategy and support the United States Armed Forces. This policy guidance is intended to provide flexibility, responsiveness, innovation, discipline and a streamlined management system. Therefore, the DoDD 5000.2 policy guidance prescribes, "Responsibility for the acquisition of systems shall be decentralized to the maximum extent practicable." A newly transformed DISA demonstrates the DISA's efforts to improve all acquisition within the DISA. The DISA has established a strong Program Executive Officers-like structure to conduct day-to-day acquisition oversight of acquisition activities and support with program office planning and milestone preparation. Funding is used to provide acquisition subject matter expertise to support the CAE acquisition role for acquisition of programs, projects and services utilizing the best practices of commercial industry and government, benchmarking, analysis, and implementation.

I. Description of Operations Financed (continued): By Mission Area

- Manpower, Personnel and Security (MPS) As directed by various mandates such as, the DoD 5200.1-R (Information Security Program); DoDD 2000.16 (Antiterrorism/Force Protection Program); and DCID 6/9 (Physical Security for Sensitive Compartmented Information Facilities (SCIF); DoDD 2000.16, Anti-terrorism Program; and Government Employees Training Act; Title 5, USC, Chapter 41; Executive Order 11348; Part 410 of Title 5, CFR; Section 1112 of the National Defense Authorization Act for FY 02; and the DISA 500 Day Plan, the Manpower, Personnel and Security Directorate (MPS) funds are to develop and implement plans, programs and oversight worldwide in the areas of civilian personnel, military personnel, human resource development, organization and manpower program administration, payroll, travel, transportation, mail management, visual information, security, real estate facilities, and supply services.

- Procurement and Logistics (PLD) provides expert advice in the areas of acquisition and logistics support to the Agency. PLD ensures that there is a seamless and timely DISA procurement process that is responsive to the needs of the entire Agency. PLD provides for the procurement of global net-centric capabilities, information technology services and equipment, and provides support to customers through innovative contracting and acquisition logistics efforts. Also, PLD provides acquisition and logistics life-cycle planning and supportability for all Acquisition Category (ACAT) programs and special projects that fall under the purview of the CAE. Specific program activities include: providing acquisition solutions, strategy and planning, policy and services; promoting full and open competition; directing the Agency acquisition business development activities; and implementing automated acquisition tools, processes, and performance metrics.

As required by the DISA Acquisition Oversight Review Report dated 21 July 2003, PLD was directed to establish the Agency’s logistics policy and guidance. Efforts in this area

I. Description of Operations Financed (continued): By Mission Area

include providing acquisition life cycle logistics planning; providing Integrated Acquisition Logistics support to the DISA's strategic business units; identifying supportability objectives and rules of engagement for the DISA's organizations; and participating in Integrated Product Teams (IPTs) and Integrated Logistics Support Management Teams (ILSMT). Additionally, PLD is responsible for implementing automated programs, such as Past Performance Information Management System, Electronic Data Management System (EDMS) and Enterprise Business Modernization Program, which support congressionally mandated acts such as the Government Paperwork Elimination Act of 1998 and the Clinger-Cohen Act of 1996. Decrease beginning in FY 2008 reflects a change proposal to convert PL from an appropriated to a Defense Working Capital Fund (DWCF) activity.

- Strategic Planning and Information (SPI) The Chief Information Office and Strategic Planning and Information Directorate (SPI) supports the Director, DISA, in decision-making; strategy-development and communicating that strategy both internally and externally; aligning the DISA program execution with Department of Defense (DOD) in planning, engineering, acquiring, fielding, and supporting global net-centric solutions; operating the DISA Information System Network; information assurance and management of the DISA information technology resources. As a shared services unit, SPI supports the DISA missions with cost-effective information tools and capabilities and provides leadership and support in a wide range of Agency and DOD information management initiatives.

SPI directs IT policy development and promulgation in the DISA and provides Agency oversight for IT systems. SPI leads the Agency in developing its enterprise architecture and internal IT Enterprise applications; conducting IT capital investment planning; and overseeing records management. Additionally, SPI supports the DISA's strategic

I. Description of Operations Financed (continued): By Mission Area

objectives by providing Information Assurance (IA) support. IA services include but are not limited to: certification and accreditation support, Federal Information Security Management Act (FISMA) and Information Assurance Vulnerability Alert (IAVA) management, Public Key Infrastructure support and IA planning and policies formulation. SPI is also responsible for leading, advising, and facilitating the transformation of the DISA into a knowledge-enabled, process-oriented, and customer-focused organization.

The Director, DISA, directed the organization to deploy an agency-wide 'world-class' network. In keeping with this mandate, the DISANet supports the DISA with secure and seamless connectivity across all DISANet sites and provides adequate bandwidth to support mission requirements in both classified and unclassified domains. SPI operates and maintains the DISA's Information Systems Center (DISC), including automated information networks, voice (telephone) systems, video teleconferencing systems, and other DISA information support centers. Funds provide operational network support in both the classified and unclassified environments for over 8,500 DISA employees and contractors in 35 locations worldwide (8 National Capital Region (NCR), 15 Continental United States, and 12 Outside the Continental United States). This entails all aspects of planning, procuring, systems integration, installation, and operation and maintenance of the local area networks in support of the DISA internal/external customers including OSD and the Joint Staff.

SPI develops the Critical Infrastructure Protection (CIP) and Information Assurance (IA) Integration CONOPS (processes and procedures for integration of the logical (cyber) and physical views of the GIG to enhance situational awareness of mission-critical GIG assets;) conducts prototype GIG asset Vulnerability Assessments to validate methodology; assures data standardization, compliance, and interoperability of CIP IT Systems; and identifies GIG critical assets.

I. Description of Operations Financed (continued): By Mission Area

SPI also provides the DISA a worldwide Continuity of Operations (COOP) Program in accordance with DOD Directives and Executive Branch national guidance. Specifically, SPI maintains and improves the functionality of the DISA relocation facilities; reviews, rewrites, staffs, publishes, and implements the DISA COOP plans and policies; integrates the DISA COOP program with all Mission Assurance program elements; and funds maintenance and support for existing COOP/Data Replication infrastructure. FY 2009 funds support operations for the DISANet World-wide as well as life cycle at the DISA Continuity of Operations program sites.

In addition, SPI manages the DISA's Knowledge Management (KM) project, which is both a DISA transformation initiative and a Government-wide initiative related to the management of human capital. The President's Management Agenda in FY 2002 required organizations to "adopt information technology systems to capture some of the knowledge and skills of retiring employees." The DISA's KM initiative will help generate, capture, integrate, and disseminate information and knowledge that is relevant to the DISA's mission. The key technology supporting the DISA's KM Program is the Enterprise Data and Global Exchange (EDGE) portal, which is governed by a formal management structure and a set of interrelated initiatives that are supported by senior leadership. Evolution of EDGE capabilities is being performed in four phases. Phase 1 focused on establishing a working prototype for approximately 500 users in an unclassified environment. Phase 2 focused on integrating key information sharing applications into the EDGE and increasing the user population of the prototype to approximately 3000 users. Funding in FY 2008 supports Phase 3 is focused on deploying the EDGE Agency-wide in an unclassified environment, establishing a classified instance of the portal, providing a customer view into EDGE data, and refining/enhancing capabilities by capitalizing on lessons learned from the prototyping phases. Phase 4 will be focused on more advanced knowledge management capabilities such as business intelligence, data mining, expert systems,

I. Description of Operations Financed (continued): By Mission Area

intelligent agents, etc. that will allow us to more easily exploit the tacit knowledge embedded in the minds of Agency personnel.

6. Special Missions: Reliable, robust, and redundant communication and information systems are critical to positive control over U.S. Armed Forces. The DISA plans, develops, and supports Command, Control, and Communications (C3) that serve the needs of the President and the Secretary of Defense under all conditions of peace and war. The Special Mission Activity provides operational telecommunications and other related support to the President of the United States, the Vice President, the First Lady, the United States Secret Service (USSS), the Executive Office of the President, the White House Staff, the National Security Council (NSC), the White House Press Office, the White House Military Office (WHMO), the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and others by direction. These activities consists of several sub-activities: White House Communications Agency (WHCA) including support to the US Secret Service (USSC), White House Situation Support Staff (WHSSS), White House Support, Senior Leadership Communications System (SLCS), Crisis Management System (CMS) for formerly referred to as Secure Video Teleconferencing System (SVTS), Minimum Essential Emergency Communications Network (MEECN), and Communications Management Control Activity (CMCA). All of these sub-activities support the Commander-in-Chief (CINC) communications ranging from modern enterprise information technology to highly secure and survivable command and control of nuclear forces. The Special Mission Activity consists of:

Mission Area Component ($ in Thousands)	FY 2006 Actuals	FY 2007	FY 2008	FY 2009
a. White House Communications Agency(WHCA)	100,474	104,177	123,767	127,958
b. White House Situation Support Staff(WHSSS)	14,846	5,546	5,748	5,929

I. Description of Operations Financed (continued): By Mission Area

c. Crises Management System (CMS)	7,926	8,882	9,946	10,107
d. Minimum Essential Emergency Communications Network (MEECN)	6,548	4,919	5,577	5,721
e. Communications Management Control Activity(CMCA)	2,839	869	925	943
Special Mission Area Total	**132,633**	**124,393**	**145,963**	**150,658**

a. White House Communication Activity (WHCA)

White House Communications Agency (WHCA) is a joint service military agency under operational control of the White House Military Office (WHMO) and the administrative control of DISA. WHCA's budget for FY 2008-2009 supports operations and maintenance of items necessary to provide instantaneous secure and non-secure voice and data/record communications support to the President, the Vice President, the First Lady, the United States Secret Service, (USSS), the Executive Office of the President, the White House Staff, the National Security Council (NSC), the White House Press, WHMO, and others by direction. Based on enactment of Public Law 109-163, WHCA provides the President and Vice President audiovisual and photographic services in the NCR and at trip sites worldwide. These funds cover personnel costs and contract support costs which will support Presidential podium, master control and event switch, and other audio support. WHCA will focus its efforts in FY 2008 and FY 2009 on sustaining and refreshing communications support to the White House. The WHCA will sustain the fixed and travel missions at the high OPTEMPO levels expected in FY 2008, modernize Presidential secure communications systems to correct shortfalls in reliability and voice quality; upgrade video distribution at Presidential facilities to digital in advance of the FCC-mandated analog TV phase-out; provision communications at the next Presidential and Vice-Presidential second residences, and complete the relocation of critical communications nodes to a location outside the Washington area. In addition, WHCA will improve quality

I. Description of Operations Financed (continued): By Mission Area

and reliability of non-secure voice communications for the President and supporting staff, expand Presidential support staff's access to intelligence data, improve the Presidential support data network's reliability and survivability, and evaluate off-the-shelf solutions for Presidential communications requirements.

United States Secret Service (USSS) – The WHCA's budget supports the IT requirements for the USSS, providing information systems support to the USSS mission of protecting the President and Vice President. Approximately seventy-five percent of these funds provide wireless and telecommunications support for President, Vice President, and First Lady at trip sites; with the remainder supporting requirements in the National Capital Region (NCR); and at their private residents.

b. White House Situation Support Staff (WHSSS)

Funds provide for classified communications, computer, and intelligence systems for the National Security Advisor, White House Situation Room, the NSC staff, and other White House offices as well as information systems used by the NSC, including pay, benefits and support costs for civilian personnel. The FY 2008 budget reflects the increased cost of maintaining classified executive information systems support to the NSC.

c. Crisis Management System (CMS) (formerly Secure Video Teleconferencing System)

CMS provides state-of-the-art video teleconferencing – SVTS, Crisis Management Network (CMN), and the National Intelligence Watch Officers Network (NOIWON) to the President, Vice President, National Security Advisor, and others as directed by the National Security Council (NSC), both in fixed and mobile modes. Funding supports the cost of maintenance, life-cycle equipment replacement, and engineering support.

I. Description of Operations Financed (continued): By Mission Area

d. Communications Management Control Activity (CMCA)

CMCA resources provide support to both the USSS and the Department of Defense for special activities such as candidates in Presidential elections, Olympics, and other special events as directed. CMCA funds provide for pay, benefits and support costs for personnel, as well as minor equipment purchases and miscellaneous contract support.

e. Minimum Emergency Essential Communications Network (MEECN)

MEECN supports a highly survivable communications network capable of transmitting Single Integrated Operational Plan (SIOP) messages and crisis conferences with the President, Vice President, Secretary of Defense, and the Chairman of the Joint Chiefs of Staff to the Combatant Commands and to deployed US nuclear forces.

These sub-activities support the Commander in Chief (CINC) communications from modern enterprise information technology to highly secure and survivable command and control of nuclear forces. Grouping these sub-activities together provides a management structure that ensures the provision of these capabilities in the White House, aboard Air Force One, in a motorcade limousine, or at Presidential appearances and trip sites. The program in FY 2007 and out is increased to support additional mission support as well as fund the maintenance of equipment acquired through supplemental resources.

II. Force Structure Summary: Optional for O&M, Defense-wide activities.

DEFENSE INFORMATION SYSTEMS AGENCY
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2008/FY 2009 Budget Estimates

III. Financial Summary ($ in thousands)

		FY 2007						
		Congressional Action						
A. BA Subactivities	FY 2006 Actuals	Budget Request	Amount	Percent	Appropriated	Current Estimate	FY 2008 Estimate	FY 2009 Estimate
4. Administrative and Service-Wide Activities								
Transition to Net Centric Environment	111,435	97,565	-3,852	-3.9%	93,713	92,807	93,339	167,412
Eliminate Bandwidth Constraints	299,280	145,713	-5,753	-3.9%	139,960	159,780	144,195	149,055
GIG Network Operations and Defense	302,499	325,072	-15,834	-4.9%	309,238	312,980	336,007	412,208
Exploit the GIG for Improved Decision Making	233,802	224,328	-8,856	-3.9%	215,472	212,799	159,538	174,330
Deliver Capabilities Effectively/Efficiently	80,490	76,305	-3,012	3.9%	73,293	78,134	66,552	64,345
Special Missions	132,633	129,635	-2,118	-1.6%	127,517	124,393	145,963	150,658
TOTAL	**1,160,139**	**998,618**	**-39,425**	**-3.9%**	**959,193**	**980,893**	**945,594**	**1,118,008**

* The FY 2006 actual column includes $40.000 thousand of FY 2006 Title IX (PL 109-289), $77.000 of FY 2006 Supplemental funds, $2.744 thousand of FY 2006 Hurricane Supplemental funds (PL 109-148), and $.500 thousand of FY 2006 Emergency Relief Fund.
* The FY 2007 Estimate column excludes $38.800 of FY 2007 Title IX obligations (PL 109-289) but includes $21.700 thousand for Spectrum Relocation Fund Activities.

DEFENSE INFORMATION SYSTEMS AGENCY
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2008/FY 2009 Budget Estimates

III. Financial Summary ($ in thousands)

B. Reconciliation Summary	Change FY 2007/FY 2007	Change FY 2007/FY 2008	Change FY 2008/FY 2009
Baseline Funding	**998,618**	**980,893**	**945,594**
Congressional Adjustments (Distributed)	-30,000	n/a	n/a
Congressional Adjustments (Undistributed)	-5,080	n/a	n/a
Adjustments to Meet Congressional Intent		n/a	n/a
Congressional Adjustments (General Provisions)	-4,345	n/a	n/a
Subtotal Appropriated Amount	**959,193**	n/a	n/a
Fact-of-Life Changes (CY to CY Only)		n/a	n/a
Subtotal Baseline Funding	**959,193**	n/a	n/a
Anticipated Supplemental	201,147	n/a	n/a
Reprogrammings		n/a	n/a
Price Changes		23,256	22,091
Functional Transfers – Spectrum Relocation Fund	21,700		
Program Changes	n/a	-58,555	150,323
Current Estimate	**1,182,040**	**945,594**	**1,118,008**
Less: Wartime Supplemental	**-201,147**		
Normalized Current Estimate	**980,893**	**945,594**	**1,118,008**

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
FY 2007 President's Budget Request		**998,618**
1. Congressional Adjustments		-39,425
a. Distributed Adjustments	-30,000	
b. Undistributed Adjustments - Unobligated Balances	-5,080	
c. Adjustments to meet Congressional Intent		
d. General Provisions		
1) Sec 8106 – Economic Assumptions	-3,193	
2) Sec 8097 - Excessive Growth in Travel and Transportation	-675	
e. Congressional Earmarks – Indian Lands Environmental Impact	-477	
FY 2007 Appropriated Amount		**959,193**
2. War-Related and Disaster Supplemental Appropriations		38,800
3. Fact of Life Changes: Functional Transfers– Spectrum Relocation Fund		21,700
FY 2007 Baseline Funding		**1,019,693**
4. Reprogrammings (requiring 1415 Actions)		
Revised FY 2007 Estimate		**1,019,693**
5. Less: Item 2, War-Related and Disaster Supplemental Appropriations and Item 4, Reprogrammings, Iraq Freedom Fund Transfers		-38,800
FY 2007 Normalized Current Estimate		**980,893**
6. Price Change		23,256
7. Functional Transfers		-23,841
a. Transfers In		
b. Transfers Out	-23,841	
1) The Defense Information Technology Contracting Office (DITCO) National Capital Region (NCR) to the Defense Wide Working Capital Fund (DWCF); DISA also allocates a share of its Shared Services costs to its DWCF components		

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
8. Program Increases		
a. Annualization of New FY 2007 Program		
b. One-Time FY 2008 Increases		
c. Program Growth in FY 2008		26,108
1) Joint Staff Support Center: Increased funding for multimedia support/Joint Staff products	6,942	
2) White House Communications Agency (WHCA) will sustain the fixed and travel missions at the high OPTEMPO levels, modernize Presidential secure communications systems to correct shortfalls in reliability and voice quality; upgrade video distribution at Presidential facilities to digital in advance of the FCC-mandated analog TV phase-out; provision communications at the next Presidential and Vice-Presidential second residences, and complete the relocation of critical communications nodes to a location outside the Washington area.	19,166	
9. Program Decreases		-60,822
a. Annualization of FY 2007 Program Decreases		
b. One-Time FY 2007 Increases		
1) Spectrum Relocation Fund (P.L. 108-494) transferred to the DISA to support Spectrum Management Transition and Spectrum Technology Test Bed Initiatives	-21,700	
2) National Military Communication System funds improvements required to implement the Ground Distributed Network for the National (Nuclear and Senior Leadership) Command and Control	-25,940	
c. Program Decreases in FY 2008		
1) Realignment among O&M program; selected programs include GIG Engineering Services ($-1,626) and Support efficiencies ($-11,556)	-13,182	
FY 2008 Budget Request		**945,594**
10. Price Change		22,091

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
11. Functional Transfers		
12. Program Increases		
a. Annualization of New FY 2008 Program		
b. One-Time FY 2009 Increases		
c. Program Growth in FY 2009		152,205
1) Information Systems Security Program (ISSP) designs and deploys proactive protections, deploys attack detection, and performs Information Assurance (IA) operations to insure that adequate security is provided. ISSP/IA implements host-based security systems at the enterprise level to include content filtering and intrusion prevention on secure networks and internet gateways as well as network access controls for classified networks	67,846	
2) Net-Centric Enterprise Services (NCES) increases sustainment efforts as NCES achieves full operability by FY 2009. Core enterprise services migrate to sustainment for Service Oriented Architecture Foundation, Content Discovery and Delivery, Enterprise Collaboration, and Enterprise Portal	57,898	
3) Global Command and Control System - Joint (GCCS-J) begins the migration of the JOSC to the DISA Defense Enterprise Computing Centers (DECC) in order to support net-centric operations. Increased funding will also provide for correction of deficiencies and problem reports and maintain the security posture of the GCCS-J system as new threats and vulnerabilities are identified	15,155	
4) Network Operations (NETOPS) – Increased contract costs for management and operation of worldwide communications network expanded by Global Information Grid Bandwidth Expansion	7,565	
5) White House Communications Agency (WHCA) continues to modernize Presidential secure communications systems to correct shortfalls in reliability and voice quality; upgrade video distribution at Presidential facilities	3,741	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
13. Program Decreases		-1,882
a. Annualization of FY 2008 Program Decreases		
b. One-Time FY 2008 Increases		
c. Program Decreases in FY 2009		
1) Common Operating Environment (COE) – drawdown sustainment services while continuing critical operational support. COE sustainment begins to transition to GCCS-J	-1,882	
FY 2009 Budget Request		**1,118,008**

IV. Performance Criteria and Evaluation Summary

DISA's principal approach to performance-budget integration and performance measurement is budgeting to our strategies and using a balanced scorecard (BSC) to manage and execute our strategies. The BSC also provides the "pyramid" of outcomes structure, with top-level goals, supported by strategies. Next down on the pyramid, the higher-level strategies have outcome-oriented as well as output measures, with targets, and the customer focused goal and strategies are at the top. Targets are at a level that promotes continuous improvement. The customer perspective strategies and measures are supported by financial, internal process, and learning and growth perspective strategies and measures. Top corporate level, or Level 1 strategies and measures, are supported by lower level strategies and measures developed by subordinate organizations.

BSC initiatives associated with each strategy are the means for attaining the performance desired, and metrics illustrate whether the targets for each goal has been achieved. Initiatives are resourced (e.g., funded) and have or are associated with a schedule. Scorecard owners brief the DISA senior leadership quarterly on their progress in executing their strategy. The reviews have proven invaluable in that they provide an opportunity to discuss strategy and obtain an integrated view of Agency performance. They also strengthen individual accountability and ensure alignment with Corporate-level priorities.

DISA also uses other measurement methodologies to measure performance that are integrated with budget. One example is readiness metrics and supporting data to measure readiness to execute mission essential tasks captured under the DoD Readiness Reporting System (DRRS) required by DoD Directive 7730.65. Strategies are developed for rectifying readiness deficiencies, and these strategies are addressed in program/budget planning as DoD Directive 7730.65 requires. Another example of measurement is performance and budget information for Capital Asset Plan; Business Case Summary Exhibit 300's required by the

IV. Performance Criteria and Evaluation Summary

Office of Management and Budget Circular A-11 establishes policy for the DISA's major information technology (IT) investments.

DISA has recently updated its strategy, and the new strategy addresses the need for the DISA to aggressively lead in five areas: speed to deliver IT capabilities and services faster; power to the edge to push enterprise services to the edge; operational excellence to accelerate operational effectiveness and efficiency; sharing and defense of information to enable sharing of information while staunchly protecting it; and best value - customers know and understand the value of the DISA capabilities and services. The DISA is currently updating the BSC goals, strategies, measures, and initiatives below for the new strategy.

The text below provides the DISA's existing BSC top-level goals, the strategies for the customer perspective, the linkage to the 2006 Quadrennial Defense Review (QDR) as well as the March 2005 National Defense Strategy, the DoD risk management framework (2001 QDR), *DoD Performance and Accountability Report (PAR*) for FY 2005, the *President's Management Agenda (PMA)*, and the DISA's new strategy. The QDR 2006 linkages are primarily mapped to the "Reorienting Capabilities and Forces" section of the 2006 QDR. This text below shows that the DISA's performance budget is aligned to DOD's performance budget. The text below also displays for the DISA's customer perspective strategies select performance metrics and provides a brief evaluation and assessment of select key results through the first part of FY 2006 used by the DISA to support ongoing strategic and tactical decision-making. Similar information is managed for the other perspectives, and other DISA perspective strategies and measures track to DOD PAR strategies and measures, such as civilian recruiting cycle time. The DISA's first implementation of the performance budget based on the BSC occurred with the FY 2006 budget. Select performance data by b activity Group (SAG) is presented below.

IV. Performance Criteria and Evaluation Summary

DISA's top-level goals:

- DISA Strategic Goa1 1: Enable the net-centric force (customer perspective)
- DISA Strategic Goa1 2: Build confidence in the DISA's financial stewardship (financial perspective)
- DISA Strategic Goa1 3: Improve planning, engineering, acquiring, fielding, supporting, and operating innovative net-centric services and solutions (Internal process perspective)
- DISA Strategic Goa1 4: Become the employer of choice for outstanding people with the right skills (learning and growth perspective)

Strategies for the DISA Strategic Goa1 1: Enable the net-centric force:

Corporate Strategy C-1: Transition to a net-centric environment to transform the way DoD shares information by making data continuously available in a trusted environment

- Activity Group: Transition to Net-centric Environment
- Measure: % (percent) of capabilities incorporating net-centric attributes
  - Targets and evaluation and assessment of results: New measure. Target goals of 80 to 100 percent, depending upon the portfolio. The investments on the list of eligible programs are all on track.

IV. Performance Criteria and Evaluation Summary

- Note: This strategy includes initiatives such as the execute of the Net-Centric Enterprise Services (NCES) program; the stand-up of the Net-Enabled Command Capability (NECC) Joint Program Executive Office (JPEO) as a major step towards moving Joint command and control towards a net-centric environment; to implement applicable portions of the DOD Net-Centric Data Strategy; to develop managed

- Services concept for both processing power and storage; and to plan for transition of applications and operating systems to IPv6.

  C-1 Linkages:
  - *National Defense Strategy:* Strengthen intelligence; Operating from the global commons; and conducting network-centric operations.
  - QDR: Achieving Net-Centricity, Joint Command and Control, and Defending the Homeland in Depth.
  - Risk Management Framework: Operational, Future Challenges, and Institutional Risk.
  - DoD PAR FY 2005 Strategic Goal/ Performance Goal/ Metric: Strategic Goal 4: Balancing Future Challenges Risks - execute future missions successfully against an array of prospective challengers/ Performance Goal 4.1 - Define and develop transformational capabilities
    - o Metric 4.1.2 Make Information Available on a Network that People Depend On and Trust./ Number of systems that support the Internet Protocol Version 6 (IPv6) and Number of systems that meet information assurance standards
    - o Metric 4.1.4 Populate the Network with New, Dynamic Sources of Information to Defeat the Enemy/ Percentage of DoD information available via net-centric solutions.

IV. Performance Criteria and Evaluation Summary

- President's Management Agenda (PMA): Expanded Electronic Government (expanded electronic government with the warfighter and other DOD employees and industry as the "citizen customer")
- DISA's new strategy: The DISA's new strategy still adopts the Department's vision and Strategy for new-centric operations and warfare.

Corporate Strategy C-2: Build and sustain a GIG transport infrastructure that eliminates bandwidth constraints and rapidly surges to meet demands, wherever needed

- Activity Group: Eliminate Bandwidth Constraints

- Measure: Number of circuits transitioned to new core and number of circuits discontinued
  - Targets and evaluation and assessment of results: New measure. The plan is to transition 10,000 circuits over 3 years, and over 2,775 have been transitioned.

- Note: This strategy includes initiatives such as to plan for providing bandwidth for re-basing in Europe; to develop the Service Delivery Node concept; and to plan to transition communication networks to IPv6.

  C-2 Linkages:
  - *National Defense Strategy:* Operating from the global commons; Conducting network-centric operations.
  - QDR: Achieving Net-Centricity, Joint Command and Control, and Shaping the Choices of Countries at Strategic Crossroads.
  - Risk Management Framework: Operational and Future Challenges.

IV. Performance Criteria and Evaluation Summary

- DoD PAR FY 2005 Strategic Goal/ Performance Goal/ Metric: Strategic Goal 4: Balancing Future Challenges Risks - execute future missions successfully against an array of prospective challengers/ Performance Goal 4.1 Define and develop transformational capabilities.
  - o Metric 4.1.2 Make Information Available on a Network that People Depend On and Trust/ Number of systems that support the Internet Protocol Version 6 (IPv6) and Number of systems that meet information assurance standards
  - o Metric 4.1.4 Populate the Network with New, Dynamic Sources of Information to Defeat the Enemy/ Percentage of DoD information available via net-centric solutions.
- President's Management Agenda (PMA): Expanded Electronic Government
- DISA's new strategy: The DISA's new strategy leadership areas of power to the edge to push enterprise services to the edge and operational excellence to accelerate operational effectiveness and efficiency map most closely.

Corporate Strategy C-3: Provide NetOps technical expertise and integrated solutions for GIG network operations and defense.

- Activity Group: Operate and Defend the GIG

- Measure: % of NetOps criteria achieved
  - o Targets and evaluation and assessment of results: New measure. Target of just over 60% was met or exceeded for both the second and third quarters of FY 2006. Target increases to 90% over the next four quarters.
- Measure: % completion implementing Net Common Operational Picture
  - o Targets and evaluation and assessment of results: Target of 92% for Spiral I implementation was at 80% for the most recently reported quarter (3FY06).

IV. Performance Criteria and Evaluation Summary

- Note: This strategy includes initiatives such as to support the Joint NetOps Concept of Operations (CONOPS) for the Global Information Grid (GIG).

  C-3 Linkages:
  - *National Defense Strategy*: Operating from the global commons; Conducting network-centric operations.
  - QDR: Tailored Deterrence/ New Triad and Defeating Terrorist Networks.
  - Risk Management Framework: Operational and Future Challenges.
  - DoD PAR FY 2005 Strategic Goal/ Performance Goal/ Metric: Strategic Goal 4: Balancing Future Challenges Risks - execute future missions successfully against an array of prospective challengers/ Performance Goal 4.1.
    - Metric 4.1.2 Make Information Available on a Network that People Depend On and Trust/ Number of systems that support the Internet Protocol Version 6 (IPv6) and Number of systems that meet information assurance standards
    - Metric 4.1.4 Populate the Network with New, Dynamic Sources of Information to Defeat the Enemy/ Percentage of DoD information available via net-centric solutions.
  - President’s Management Agenda (PMA): Expanded Electronic Government.
  - DISA's new strategy: The DISA's new strategy leadership area of sharing and defense of information to enable sharing of information while staunchly protecting it.

Corporate Strategy C-4 Note: During FY 2006, Corporate Strategy C-4 was combined with Strategy C-1, because of their similarity.

IV. Performance Criteria and Evaluation Summary

Corporate Strategy C-5: Deliver capabilities, based on established requirements, more effectively, economically and efficiently than we do today.

- Activity Group: Deliver Capabilities More Effectively and Efficiently

- Measure: Percentage of acquisitions capabilities that are delivered within established Acquisition Program Baselines (APB)/APB-like thresholds
  - o Targets and evaluation and assessment of results: The targets are the baselines or APB-like thresholds. Five programs with approved APBs are within their cost, schedule, and performance goals. One other program is under review as a special program that is tracked using appropriate mechanisms.

- Measure: Unit costs for services delivered
  - o Targets and evaluation and assessment of results: Four of six services with both unit cost data and targets reported costs within targets for FY 2006. One service was above the target cost because of increased customer demand resulting in a higher overall program cost. Another service was above target because of a fixed price resulting from a services contract coupled with decreased customer workload.

- Note: This strategy includes initiatives such as developing and implementing the project plan for the DISA's Base Closure and Realignment Commission (BRAC) realignment that includes the consolidation and relocation of the DISA headquarters elements in the National Capital Region to Fort Meade, Maryland.

  C-5 Linkages:
  - *National Defense Strategy:* Implementation guideline of continuous transformation.

IV. Performance Criteria and Evaluation Summary

- QDR: Toward A New Defense Enterprise.
- Risk Management Framework: Operational and Institutional Risk.
- DoD PAR FY 2005 Strategic Goal/Performance Goal/ Metric:
  - Strategic Goal 3: Balancing Institutional Risk – Align the organization and its resources to support the warfighter/ Performance Goal 3.3 - Realign Support to the Warfighter.
    - Metric 3.3.1: Reduce Customer Wait Time (Days)
    - Metric 3.3.2: Reduce Major Defense Acquisition Program Annual Rate of Acquisition Cost Growth
    - Metric 3.3.3: Reduce Major Defense Acquisition Program Acquisition Cycle Time
    - Metric 3.3.4: Reduce Major Defense Acquisition Program Operating and Support Cost Growth
  - Strategic Goal 3: Balancing Institutional Risk – Align the organization and its resources to support the warfighter/ Performance Goal 3.4 - Streamline the Decision Process, Improve Financial Management, and Drive Acquisition Excellence.
    - Metric 3.4.1: Support Acquisition Excellence Goals
- President’s Management Agenda (PMA): Budget and performance integration.
- DISA's new strategy: The DISA's new strategy leadership area of best value - customers know and understand the value of the DISA capabilities and services and the area of operational excellence to accelerate operational effectiveness and efficiency.

DEFENSE INFORMATION SYSTEMS AGENCY
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2008/FY 2009 Budget Estimates

V. Personnel Summary	FY 2006	FY 2007	FY 2008	FY 2009	Change FY 2006/ FY 2007	Change FY 2007/ FY 2008	Change FY 2008/ FY 2009
Active Military End Strength - Total	1636	1501	1465	1459	-135	-36	-6
Officer	393	358	344	343	-35	-14	-1
Enlisted	1243	1143	1121	1116	100	-22	-5
Reserve Drill Strength (E/S) – Total	198	103	93	93	-95	-10	0
Officer	70	61	51	51	-9	-10	0
Enlisted	128	42	42	42	-86	0	0
Reservists on Full Time Active Duty (E/S)	2	2	2	2	0	0	0
Officer	1	1	1	1	0	0	
Enlisted	1	1	1	1	0	0	0
Civilian End Strength –Total	2727	2483	2413	2413	-244	-70	0
U.S. Direct Hire	2643	2378	2308	2308	-265	-70	0
Total Direct Hire	2643	2378	2308	2308	-265	-70	0
Foreign National Indirect Hire	5	5	5	5	0	0	0
Memo: Reimbursable Civilians Included	79	100	100	100	21	0	0
Active Military Average Strength – Total	1636	1501	1465	1459	-135	-36	-6
Officer	393	358	344	343	-35	-14	-1
Enlisted	1243	1143	1121	1116	100	-22	-5
Reserve Drill Strength (A/S) - Total	198	103	93	93	-95	-10	0
Officer	70	61	51	51	-9	-10	0
Enlisted	128	42	42	42	-86	0	0
Reservists on Full Time Active Duty Total	2	2	2	2	0	0	0
Officer	1	1	1	1	0	0	0
Enlisted	1	1	1	1	0	0	0
Civilian FTEs (Total)							
U.S. Direct Hire	2575	2255	2217	2217	-320	-38	0
Total Direct Hire	2575	2255	2217	2217	-320	-38	0
Foreign National Indirect Hire	5	5	5	5	0	0	0
Memo: Reimbursable Civilians Included	77	75	85	85	-2	10	0
Average Annual Civilian Salary ($)							

DEFENSE INFORMATION SYSTEMS AGENCY
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2008/FY 2009 Budget Estimates

OP-32 Line	*FY2006 Actuals	Change FY 2006/FY 2007 Price	Change FY 2006/FY 2007 Program	**FY2007 Estimate	Change FY 2007/FY 2008 Price	Change FY 2007/FY 2008 Program	FY2008 Estimate	Change FY 2008/FY 2009 Price	Change FY 2008/FY 2009 Program	FY2009 Estimate
Executive, General and Special Schedules	286,167	6,939	-34,645	258,461	7,236	-14,235	251,462	6,223	-9,061	248,624
Wage Board	59	1	1	61	0	-1	60	0	1	61
Disability Compensation	867	0	229	1,096	0	57	1,153	0	58	1,211
Total Civilian Personnel Compensation	**287,093**	**6,940**	**-34,415**	**259,618**	**7,236**	**-14,179**	**252,675**	**6,223**	**-9,002**	**249,896**
Travel of Persons	29,718	713	9	30,440	700	13,023	44,163	972	-13,182	31,953
Total Travel	**29,718**	**713**	**9**	**30,440**	**700**	**13,023**	**44,163**	**972**	**-13,182**	**31,953**
Communications Services(DWCF) Tier 2	619	8	-627	0	0	0	0	0	0	0
Pentagon Reservation Maintenance	13,658	2,868	-3,248	13,278	-637	1,501	14,142	1,032	-467	14,707
Defense Finance and Accounting Services (DFAS)	8,060	-774	3,405	10,691	-513	-5,607	4,571	-242	2,362	6,691
Communcations Services (DWCF) Tier 1	18,593	502	-5,527	13,568	1,411	390	15,369	538	-1,592	14,315
Cost Reimbursable Purchases	16,650	400	-17,050	0	0	0	0	0	0	0
Total Purchases	**57,580**	**3,004**	**-23,047**	**37,537**	**261**	**-3,716**	**34,082**	**1,328**	**303**	**35,713**
Commercial Transportation	2,328	49	321	2,698	59	164	2,921	61	175	3,157
Total Transportation	**2,328**	**49**	**321**	**2,698**	**59**	**164**	**2,921**	**61**	**175**	**3,157**
Rental Payments to GSA Leases (SLUC)	19,232	481	258	19,971	499	-3,264	17,206	430	1,689	19,325
Purchased Utilities (non-DWCF)	2,684	64	140	2,888	66	386	3,340	73	140	3,553
Purchased Communications (non-DWCF)	35,591	854	-7,246	29,199	672	471	30,342	668	2,774	33,784
Rents (non-GSA)	346	8	-202	152	3	-40	115	3	-3	115
Postal Services (USPS)	189	0	76	265	0	-37	228	0	7	235
Supplies & Materials (non-DWCF)	10,633	108	-3,485	7,256	167	263	7,686	167	153	8,006
Printing & Reproduction	231	6	95	332	8	-51	289	6	0	295
Equipment Maintenance by Contract	537,721	12,914	-78,028	472,607	10,870	-54,834	428,643	9,430	152,229	590,302
Facility Maintenance by Contract	16,134	387	-4,797	11,724	270	-1,218	10,776	237	365	11,378
Equipment Purchases (non-DWCF)	54,181	1,300	-25,677	29,804	685	4,390	34,879	767	5,440	41,086
Contract Consultants	0	0	1,328	1,328	31	-45	1,314	29	-28	1,315
Management and Professional Support Services	0	0	311	311	7	-73	245	5	3	253

DEFENSE INFORMATION SYSTEMS AGENCY
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2008/FY 2009 Budget Estimates

OP-32 Line	*FY2006 Actuals	Change FY 2006/FY 2007 Price	Change FY 2006/FY 2007 Program	**FY2007 Estimate	Change FY 2007/FY 2008 Price	Change FY 2007/FY 2008 Program	FY2008 Estimate	Change FY 2008/FY 2009 Price	Change FY 2008/FY 2009 Program	FY2009 Estimate
Studies, Analyses, Evaluation	1,170	28	-802	396	9	-108	297	7	1	305
Engineering Technical Services	3,042	164	-556	2,650	63	-171	2,542	60	287	2,889
Locally Purchased Fuel (non-DWCF)	28	4	-32	0	0	0	0	0	0	0
Other Intra-governmental Purchases	19,314	464	-576	19,202	442	-1,357	18,287	402	-551	18,138
Grants/Subsidies/Contributions	17	0	30	47	1	-9	39	1	0	40
Other Contracts	82,757	1,986	-32,318	52,425	1,206	1,850	55,481	1,221	9,523	66,225
Other Costs	150	4	-111	43	1	0	44	1	0	45
Total Other Purchases	**783,420**	**18,772**	**-151,592**	**650,600**	**15,000**	**-53,847**	**611,753**	**13,507**	**172,029**	**797,289**
Total Activity Group	**1,160,139**	**29,478**	**-208,724**	**980,893**	**23,256**	**-58,555**	**945,594**	**22,091**	**150,323**	**1,118,008**

* The FY 2006 Actual column includes $.500 thousand of FY 2006 Hurricane Supplemental funds (PL 108-324, PL 109-61, and PL 109-62), $77.000 thousand for Global War on Terrorism supplemental obligations, and $40.000 thousand of FY 2006 Title IX obligations (PL 108-287).
** The FY 2007 Estimate column excludes $38.800 million of FY 2007 Title IX, Global War on Terrorism (PL 109-289) and includes $21.700 million for Spectrum Relocation Fund.