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

February 2008

(This page intentionally left blank.)

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

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

	FY 2007 Actuals	Price Change	Program Change	FY 2008 Estimate	Price Change	Program Change	FY 2009 Estimate
DISA	1,096,144	21,477	-173,035	944,586	21,897	261,143	1,227,626

* The FY 2007 Actual column includes $28,000 thousand of FY 2007 Global War on Terror Emergency Supplemental funds (PL 110-28), $56,939 thousand of Iraq Freedom Fund transfers, $38,600. thousand of FY 2007 Title IX funds (PL 109-289), and $2,900 of Spectrum Relocation funds.
** The FY 2008 Estimate column includes $18.919 million of X-year funding for Spectrum Relocation, excludes $44,510 thousand of GWOT funds received from the Consolidated Appropriations Act of 2008 (HR 2764/PL 110 – 15) out of the total GWOT request of $175,000 thousand.

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 Department of Defense (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. Net-centricity will create 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 so that operational agility is enabled. It is a world in which the U.S. military can freely exchange information routinely with coalition partners and others responsible for national security and defense.

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 (C4) Systems in support of peacetime, contingency, war or other crisis;
- Supporting contingency and wartime planning with the Joint Staff and the Combatant Commands (COCOMS);
- 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 U.S. Strategic Command (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;
- Protecting the 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;

I. Description of Operations Financed: (continued)

- Maintaining human resource initiatives to retain and reshape the DISA workforce to meet future requirements, increase quality and technical depth, and support upcoming challenges.

The DISA is organized and structured in support of DoD's strategic framework to incorporate the goals and objectives in the Performance Improvement Initiative (PII); address customer requirements and priorities; and implement the DoD and 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.

The 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 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.

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.

I. Description of Operations Financed: (continued)

4. **Transition to DoD enterprise-wide capabilities** for communities of interest, such as command and control, and 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 DISA's critical special mission to support the Commander in Chief.

The DISA continues to use the Total Cost Allocation Model that assigns costs of shared services to products and services. The Cost Allocation Model identifies the total cost of a program and avoids unintended subsidy to the Defense Working Capital Fund and gains visibility and insight into cost and consumption of shared services and addresses efficiencies.

Significant Program Changes:

The FY 2009 budget reflects the 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 different NCES core enterprise services, as they migrate from a developmental stage, to an operational stage. Milestone C is on target to occur in FY 2008 with as scheduled Initial Operational Test and Evaluation (IOT&E) occurring late in FY 2008. Upon completion of IOT&E, a Full Deployment Decision Review (FDDR) will determine the readiness of NCES services to migrate to operational status/capability for Service Oriented Architecture Foundation, Content Discovery and Delivery, Collaboration, and User Access (Portal). In FY 2009, NCES will expand the infrastructure and license support of Knowledge Online requirements beyond the current 2 million user limit to 3.5 million users, 75 percent increase in user capacity. Knowledge Online provides a single port for DoD user access to NCES and provides a personalized, user-defined, web-based presentation provides for secure access to enterprise services.

Information Systems Security Program (ISSP)/Information Assurance (IA): The DISA continues to focus on designing and deploying proactive protections, deploying attack detection, and performing IA operations to ensure adequate security is provided. In FY 2009, ISSP/IA will field additional Demilitarized Zones (DMZs) on the Non-secret Internet Protocol Router Network (NIPRNet), expand the Enterprise Cross Domain Service (CDS), support Joint Enterprise Directory Service (JEDS) on the Secret Internet Protocol Internet Router Network (SIPRNet), field additional SIPRNet firewalls, increase by 50 the number of IA assessments to determine compliance with IA policies, and develop increased and improved IA training for System Administrators (SA) and users. ISSP/IA will deploy additional enterprise-wide tools for SIPRNet Network Access Control (NAC), Authentication & Privilege Management, correlation and analysis of CND events, content filtering at the NIPRNet to Internet boundary and identification of Insider Threats. In addition, ISSP/IA will continue accelerated deployment of Host-Based Security System (HBSS) on the SIPRNet and NIPRNet networks.

I. Description of Operations Financed: (continued)

Global Command and Control System – Joint (GCCS-J): The DISA is executing functional transfers: (1) from the GCCS-J to the Joint Staff Support Center (JSSC) local mission funding (National Military Command System (NMCS) program); and (2) the legacy Common Operating Environment sustainment activities (GIG Engineering Services program) into the GCCS-J program. FY 2009 funding will support the sustainment of the GCCS-J Block V version releases (GCCS-J v4.1 and GCCS-J v4.2) used by the warfighter until such time as NECC's capabilities are available for use. In addition, FY 2009 funding will be used to begin the migration of the JSSC to the DISA Defense Enterprise Computing Centers (DECC) in order to support net-centric operations. The GCCS-J will correct deficiencies and problem reports, and maintain the security posture of the GCCS-J system as new threats and vulnerabilities are identified.

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 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 projected; 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; provide 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.

I. Description of Operations Financed: (continued)

Comprehensive National Cybersecurity Initiative: The DISA and the JTF-GNO will provide support to the Federal Government's response to the cyber security threat through this Initiative.

Combined Enterprise Regional Information Exchange System (CENTRIXS): The DISA/Multi-National Information Sharing (MNIS) Joint Program Office (JPO) will transition services and capabilities of CENTRIXS and Griffin (enables sharing of classified information between coalition partners) into centralized operations.

- The CENTRIXS will provide a combination of separate multilateral and bilateral networks that will allow the U.S. and coalition forces to securely share mission specific information.
- The CENTRIXS Cross Enclave Requirement (CCER) will enable warfighters to efficiently share time critical information with coalition partners; reduce timeline to add new Communities of Interest (COI); and establish a common suite of information sharing services to all mission partners with controlled access to Command and Control (C2)/Intelligence applications based on country trust and user role.
- Griffin will enable the sharing of classified information with Allies between national classified networks and Command and Control systems using current capabilities.
- The Combined Federated Battle Laboratory Network (CFBLNet) will provide multinational infrastructure and services to support the evaluation and resolution of combined Command, Control, Communications, Computers, Intelligence and Surveillance Reconnaissance (C4ISR) interoperability shortfalls.

I. Description of Operations Financed: (continued)

- The CFBLNet will enable member nations to conduct initiatives to improve coalition information exchange capabilities, experiment with emerging capabilities and resolve deficiencies in existing applications, systems or equipment.

Net-Enabled Command Capability (NECC): The DoD realigned funding to NECC in FY 2009, to support and maintain fielded C2 capabilities as described below. Funds will provide hardware/software license and maintenance costs, security enhancements, training, travel, and onsite functional and technical support to assist users with new C2 capabilities. Funds maintain operational security (i.e., managing and implementing security patches in response to Information Assurance Vulnerability Alerts, supporting Security Test & Evaluations to maintain the Authority to Operate, and supporting Security Readiness Reviews) at the NECC Joint Technical Operations Control Capability (JTOCC). In addition, funds will be used for the Defense Enterprise Computer Center (DECC) hosting costs. Funds will be used for the maintenance of the Federated Development and Certification Environment (FDCE) which includes hardware, software and COTS applications. The FDCE is a virtual environment accessible through the network. Warfighters, developers, testers, engineers, certifiers and all other program personnel use the FDCE to assess and manipulate the NECC products which are C2 capability modules (CMs) residing on the Global Information Grid (GIG).

Narrative Explanation of Changes – FY 2008 to FY 2009: The total net change between FY 2008 and FY 2009 is +$283,040 thousand (+$21,897 thousand in Price Change and +$261,143 thousand in Program Change). This change includes internally realigned DoD funding into the NECC Program to provide for a single, integrated, coherent system for operational level C2 ($27,113 thousand); increased Information Systems Security/Information Assurance funding to ensure adequate security is provided to the network and other program adjustments ($176,897); funding for CENTRIXS efforts to consolidate networks for coalition partners that will allow the secure sharing of mission

I. Description of Operations Financed: (continued)

specific information ($16,000 thousand); an increased in O&M funding for NCES as it transitions from RDT&E to full operational capability in FY 2009 and adds defense users to Knowledge Online ($7,600 thousand); provides funding for upgrades in Presidential communications systems($1,100 thousand); increased in funding to support the DISA computer hosting costs ($14,300 thousand); and funding to supports classified activities such as the Comprehensive National Cybersecurity Initiative ($36,000 thousand).

Descriptions of Operations Financed by Mission Area:

1. Transition to Net-Centric Environment: The ability to conduct network-centric operations is central to DoD'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 of fielding Increment One capabilities in FY 2008. The following programs comprise the Transition to Net-Centric Environment mission area:

Mission Area Component ($ in Thousands)	FY 2007	FY 2008	FY 2009
a. Net-Centric Enterprise Services	32,831	26,595	89,897
b. Global Information Grid Engineering Services	49,209	54,798	72,993
c. Advanced Concept Technology Demonstration	8,678	4,757	5,759
d. Coalition Warrior Interoperability Demonstration	1,712	2,145	2,201
e. Other Programs	2,053	0	0
Transition to Net Centric Environment Total	**94,483**	**88,295**	**170,850**

a. Net-Centric Enterprise Services (NCES): The DoD is transforming the way it conducts warfare, business operations, and enterprise management. As part of this transformation,

I. Description of Operations Financed: (continued)

the Department has embraced the concept of Net-Centricity, a robust, globally interconnected, network environment (including infrastructure, systems, processes, and people) in which data is shared in a timely and seamless way among users, applications, and platforms during all phases of warfighting efforts. Net-Centricity enables substantially improved situational awareness, significantly shortened decision-making cycles, and better asset protection. The NCES is the foundation and one of the catalysts for transforming the current DoD environment to a dynamic, collaborative, information sharing environment.

The NCES is the DoD wide initiative to develop shared underpinning capabilities for future joint warfighting through a capabilities-based joint force. The NCES will support a transformed joint force that is fully integrated, networked, decentralized, adaptable, capable of decision superiority, and lethal. The NCES will serve as one of the catalysts to enable the DoD's transition to an environment where all data is tagged and rapidly searchable by authorized users and applications.

Although NCES must support an expanding number of programs of record, enterprise capabilities will initially be made available to the DoD, Federal, and authorized Coalition users that are serviced by the Defense Information Systems Network (DISN) Secret Internet Protocol Routed Network (SIPRNET). Initial capabilities will not support all operational and tactical users beyond the DISN, but NCES will provide services that those users can access, commensurate with available transport, doctrine, and the Commander's Intent for bandwidth usage and information policy. The NCES will continue to expand and refine services that will support a larger segment of operational and tactical users in bandwidth restricted, intermittent, and disconnected environments.
The NCES program will lay the foundation on which to begin closing capabilities gaps identified in the Joint Vision 2020. Five documents, the NCES Warfighter Concept of

I. Description of Operations Financed: (continued)

Operations (CONOPS), GIG Mission Area (MA) Initial Capabilities Document (ICD), the GIG Engineering Services (ES) ICD, the 13 April 2007 Net-Enabled Command Capability (NECC) Capability Development Document (CDD), and the Joint Capabilities Document (JCD) for Net-Centric Operational Environment (NCOE), identified gaps in the capabilities supporting timely, secure, and agile information exchange. Analysis of the capability gaps can be grouped in six high-level categories: system interoperability, collaboration, information access, cross-domain security, information exchange, and system responsiveness.

The NCES will address these gaps through the delivery of eleven core enterprise services that enhance existing information superiority capabilities and connect data with service providers and users. These eleven core enterprise services are:

1. Enterprise Service Management (ESM)
2. Machine-to-Machine Messaging (M2M Messaging)
3. Service Discovery
4. People Discovery
5. Metadata Services
6. Mediation
7. Information Assurance/Security (IA)
8. Content Discovery
9. Content Delivery
10. Collaboration
11. User Access (Portal)

These core enterprise services are necessary to provide a common information environment infrastructure that will maximize sharing, reuse, and interoperability of services; and are critical and required for net-centricity and cannot otherwise be provided by existing

I. Description of Operations Financed: (continued)

stove-pipe systems in a timely, scalable, or reusable manner. These eleven core enterprise services are organized into four product lines:

1. Service Oriented Architecture Foundation (SOAF)
2. Content Discovery and Delivery (CD&D)
3. Collaboration
4. User Access (Portal)

(1) SOAF represents the core set of system components that will provide the essential elements of interoperability, access, security, and performance. SOAF will empower service users and producers to rapidly construct and deploy interoperable service-based applications. SOAF capabilities provide the critical NCES foundational capabilities that will enable community of interest (COI) users to securely discover, share, and process information and services from a multitude of sources. The SOAF will provide the engineering flexibility necessary to respond to changing business processes and requirements.

(2) CD&D will provide search and discovery functionality across the GIG Enterprise. CD&D provides the methodology, specifications, user interfaces, and services to support advertising, discovery, and efficient delivery of information. Content Delivery provides computing infrastructure services for dynamically caching, forward staging and storage of information within the network.

(3) Collaboration provides users with a tool suite of collaboration capabilities (e.g., IM/chat and web conferencing, application sharing, whiteboarding including annotations, and application broadcasting) that meets the warfighter’s operational requirements. The

I. Description of Operations Financed: (continued)

web-accessible services will enable information sharing and processing anywhere and at anytime by any user with privileges on the DoD network.

(4) User Access to NCES Services capability will provide the user with a secure web-based access to NCES and will provide a single launch point to access NCES services, but will not be the only method used to access NCES services. The User Access to NCES Services capability will provide a flexible profiling and customization capability for capturing, managing, and acting on a full array of user preferences.

The NCES Product services will support both information sharing and shared situational awareness and will link decision makers and system users with current, essential data to achieve increased speed of command. Managed service providers will provide and support these four product lines throughout the full life cycle via services offered from a qualified GIG Computing Node.

Force Structure Summary for Operations and Maintenance: The NCES Operation and Maintenance consists of sustaining the four NCES product lines upon successful completion of the Full Deployment Decision Review (FDDR) to include capacity growth, as defined in the NCES CPD, PMO acquisition support, general management and operating expenses, mission support, and civilian pay. In an effort to reduce and/or eliminate the potential realization of risks funds are allocated to Risk Management Support to successfully achieve Milestone C requirements.

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 FDDR. Sustainment of the four NCES product lines includes production management and hosting facility support, quality assurance, information assurance/system security

I. Description of Operations Financed: (continued)

maintenance, and help desk services. Sustainment of the product lines will be the responsibility of the managed service providers (MSPs) that support NCES capabilities. The MSPs 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 managed service providers will be responsible for full life cycle support of their services, including infrastructure investment, integration, operational support (e.g., hosting, user assistance, performance reporting, and maintenance), and technology refresh. The life cycle management support will include training and training materials (as needed), maintenance, pre-production testing service, and operational management (e.g., trouble ticketing, performance reporting, and Tier 2 and Tier 3 Help Desk support). The "life cycle" of the service will be determined by the government. 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 satisfaction of specific security requirements 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).

I. Description of Operations Financed: (continued)

4. Information Assurance/System Security Maintenance support is required for system security fixes and security system upgrades.
5. Help Desk Services include 24/7/365 availability support, call management, problem management, documentation and reporting.

In addition to product line sustainment, operational funds will support capacity growth in each product line as each service is fully integrated into the DoD enterprise environment. Capacity growth is predicted for each NCES capability and is further described in the narrative explanation of changes between years.

b. Global Information Grid Engineering Services (GIG ES): This activity includes the DISA work in the areas of Chief Technology Officer (CTO) and the Systems Engineering Center (SEC).

The CTO supports efforts that will strengthen critical 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

I. Description of Operations Financed: (continued)

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 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 COCOMS, 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 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; systems-level modeling and simulation; and, lifecycle IT standards engineering activities as the DoD's Executive Agent for IT Standards. SEC develops across-theater information awareness for COCOMS through application solutions for integrated networks, to include DoD's missions in Iraq and Afghanistan and the 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 them and with each other;

2) developing a standardized DISA systems engineering and integration process to improve systems integration across DISA for all the 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

I. Description of Operations Financed: (continued)

profiles under the Defense Information Technology Standards Registry (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 the 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 the 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 anticipates the following accomplishments for the Transition to Net-Centric Environment:

- Develop, implement and continuously improve on net-centric 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.
- 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.
- 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.
- 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)

- Assess Net-Centric Certification under JCIDS requirements to reach a level of maturity in FY 2008 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.
- Effect messaging standards transition to net-centric environment, to include tactical data links, message text formats, variable message formats, and undergo net-centric service transition and IP convergence.
- Develop the GIG technical baseline, an end-to-end (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.
- 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.

c. Advanced Concept Technology Demonstrations (ACTD): The ACTDs support the integration and demonstration of new, mature information technology (IT) and advanced operational concepts into net-centric battlespace technologies that enhance current force capabilities and project future force IT requirements. Funding is essential to ensure DISA succeeds in its mandate to deliver prioritized emergent IT capabilities and services faster, extend enterprise services to the edge, accelerate operational effectiveness and efficiency, and enable information sharing and assurance. The GIG Technology Transition Program utilizes three key mechanisms to streamline the process to field emergent

I. Description of Operations Financed: (continued)

requirements: Advanced Concept/Joint Capabilities Demonstrations (AC/JCTDs) with the Office of the Secretary of Defense (OSD)/Combatant Command/Service/Agency teaming; Joint Ventures with Combatant Command/Program of Record (POR); and, Risk Mitigation Pilots with POR and COI teaming. Feedback efforts from the operational community increase the robustness of the ultimate technology solutions. These efforts provide strategic outreach to DISA COCOMS, Service, and Agency partners to ensure our customers know and understand the value of our net-centric capabilities and services.

The GIG Technology Transition Program provides critical new customer focus on the long-term global war on terrorism via the confluence of technology, security cooperation, and education. The GIG Technology Transition Program assists in supporting and providing PORs with agile, adaptive, and capabilities-based IT while providing US forces with peacetime and contingency access. Program funding is critical to the development of system enhancements necessary to lead and partner in initiatives to build a net-centric system with the capability to rapidly adapt to changing demands. The GIG Technology Transition Program provides IT solutions and advanced concepts to address warfighter capability gaps in protecting information from interception and exploitation and delivering information in a useful format.

In support of the transformation to net-centricity, the GIG Technology Transition Program establishes a cooperative partnership with the Deputy Undersecretary of Defense for Advanced Systems & Concepts to advance contemporary doctrine, policies, and procedures that enhance combatant command objectives. The GIG Technology Transition Program engages in technical development and transition efforts associated with Network Infrastructure and NetOps.

I. Description of Operations Financed: (continued)

d. Coalition Warrior Interoperability Demonstration (CWID): The CWID is a Chairman of the Joint Chiefs of Staff's program enabling DoD, Homeland Security and coalition partners to investigate command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) solutions. CWID focuses on C4ISR objectives derived from capability gaps identified by the COCOMS and coalition partners. CWID provides a simulated, scenario driven, net-centric, operational environment to demonstrate relevant technology solutions for operational improvements and interoperability of new and legacy systems. The Demonstration provides an opportunity for warfighter, first responders, and coalition partners to exercise, observe, evaluate and validate demonstrated solutions.

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. The operational environment (simulated) is created by the host combatant command and provides the context for warfighter validation of the proposed interoperability solutions. Interoperability between communication systems is essential. C4 responsibilities may cross multiple intergovernmental boundaries. The CWID provides a forum for exploring solutions to these challenges.

CWID requires a coalition information environment that 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. The CWID will be conducted as a U.S.-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

I. Description of Operations Financed: (continued)

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 GIG.

The governing directive for CWID states that DISA will direct the daily operations for the administration, planning and execution of CWID through the formation and maintenance of a CWID Joint Management Office (JMO). The Director, CWID JMO reports on the progress and status of the CWID planning cycle and is supported by a working group structure.

2. Eliminate Bandwidth Constraints: 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, reducing key cross-cutting modeling and simulation capabilities, and limiting growth in standards activities. Included in this Mission area are:

I. Description of Operations Financed: (continued)

Mission Area Component ($ in Thousands)	FY 2007	FY 2008	FY 2009
a. DoD Teleport Program/STEP/GEMSIS	16,840	18,719	18,602
b. Defense Spectrum Organization	32,568	45,832	30,197
c. Defense Information Systems Network Enterprise Activities	170,776	86,112	91,764
d. Defense Information Systems Network Subscription	15,295	16,466	16,352
Eliminate Bandwidth Constraints Total	**235,479**	**167,129**	**156,915**

DoD Teleport: The Teleport investment is driven by requirements validated by the Joint Chiefs of Staff and is linked with DISA's core strategic goal to transition to a net-centric environment to transform the way 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 DoD Performance Improvement Initiative (PII) 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 Integration (NII) architecture. Teleport provides seamless access to the Defense Information System Network (DISN) and GIG, which supports the 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 program. Generation One will complete the initial build-out by integrating military Ka SATCOM capabilities into the Teleport system in FY 2009. Generation Two adds additional military Ka band capacity and will complete installation of Internet Protocol (IP) Net-Centric capabilities to all

I. Description of Operations Financed: (continued)

the core sites. Net-Centric communications allow for the use of IP for enhanced network interoperability and enable dynamic satellite allocation to reduce satellite lease costs and increase overall performance. Generation Two will complete in FY 2009 and provides Ka band capacity increases as well as Ka band SATCOM terminals at four sites; it will provide IP capability across the Teleport system.

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 Global Electromagnetic Spectrum Information System (GEMSIS) mission capability will respond to the Strategic Planning Guidance (SPG) and the Quadrennial Defense Review (QDR) goal of leveraging information technology. As part of planning, resourcing, acquiring, and implementing the future transformation of dynamic frequency management, GEMSIS will provide a secure and globally connected suite of spectrum management services; will be hosted on the GIG’s Enterprise Information Environment; and will be available to users as an enterprise services. The system is planned to provide a range of capabilities that will improve upon current spectrum management systems and access information from other related operational planning systems.

I. Description of Operations Financed: (continued)

On 23 January 2006, The Joint requirements oversight council (JROC) approved the GEMSIS Initial Capabilities Document (ICD). The GEMSIS is intended to provide capabilities for integrated spectrum operations across the entire DoD in addition to interoperability with federal, state, and local government spectrum agencies, and coalition forces. The GEMSIS is envisioned as a net-centric emerging capability providing commanders with an increased common picture of spectrum situational awareness of friendly and hostile forces while transparently deconflicting competing mission requirements for spectrum use. This capability will enable the transformation from the current preplanned and static assignment strategy into autonomous and adaptive spectrum operations.

GEMSIS is expected to provide a long-term solution for spectrum management capabilities. GEMSIS will provide a family of spectrum capabilities and a joint enabling concept. As a family of spectrum capabilities, GEMSIS will support all levels of warfare (strategic, operational, and tactical) through the fielding of supportable and adaptive RF spectrum-dependent capabilities. Military readiness, mobilization, strategic operations, logistics, and space-based capabilities depend on the availability of the electromagnetic spectrum to plan and execute missions. Global communications, the sustaining infrastructure, interagency, local government, and coalition operations similarly depend on spectrum planning and execution. The GEMSIS architecture will provide GIG-based capabilities enabling the seamless exchange of spectrum access resources, equipment supportability assessments, mission planning and rehearsal guidance, and acquisition decision support inputs DoD wide.

b. Defense Spectrum Organization: The DSO was established by merging and realigning the spectrum assets and resources of the DISA Defense Spectrum Office, hereafter referred to as the Strategic Planning Office (SPO), and the Joint Spectrum Center (JSC). The Joint Spectrum Center’s (JSC) mission is to ensure the DoD’s effective use of the

I. Description of Operations Financed: (continued)

electromagnetic (EM) spectrum in support of national security and military objectives. The JSC serves as the DoD technical center of excellence for EM spectrum matters in support of the Unified Commands, Joint Staff, ASD (NII), Military Departments, and Defense Agencies. The JSC supports the Electronic Protect missions of Information Warfare (IW) as they relate to spectrum supremacy. It is responsible for developing and maintaining the DoD standard information systems that support the DoD spectrum-related activities and processes. Specifically, the JSC designs, develops, and maintains the DoD automated spectrum management systems, evaluation tools, and databases employed by the Unified Commands, Military Departments, and Defense Agencies. The JSC databases are the prime sources of information for the DoD use of the EM spectrum. The JSC provides technical assistance to the Office of ASD (NII), the Joint Staff, DoD activities and the Unified Commands in support of spectrum policy decisions and ensuring the development, acquisition, and operational deployment of systems that are compatible with other spectrum-dependent systems operating within the same EM environment. The Center is the DoD focal point for technical spectrum-related support, Electromagnetic Environmental Effects (E3), and EM interference resolution assistance to operational units including deployable support to Combatant Command (COCOM) Joint Task Forces. The JSC mission is integral to other vital activities such as Information Operations (IO), Command and Control (C2) Protect, and other defensive IW activities as directed by the Joint Staff.

The Strategic Planning Office’s (SPO) mission is to provide integrated strategies, policies, processes, and practices to achieve global spectrum access for national security obligations. SPO will primarily assist the ASD (NII) with: improving EM spectrum management and E3 business processes; enhancing the current warfighter spectrum management capabilities to allow for COCOMS contingency planning; updating spectrum supportability roles and responsibilities throughout the spectrum management community; and enhancing acquisition and requirements processes to assure spectrum access.

I. Description of Operations Financed: (continued)

Additional roles include: improving future warfighter EM spectrum utilization through technological innovation by assisting in research, studying, and steering the direction of emerging technology advances into the DoD acquisition cycle allowing for greater warfighter capabilities; promoting EM spectrum and E3 awareness and education through outreach programs that ensure awareness of spectrum-related developments; advocating and defending the DoD's EM spectrum needs in national and international EM spectrum forums by developing and executing realistic allocation/reallocation strategies; proactive DoD preparation for the World Radio Communication Conference; and integrating spectrum-related technology issues in national and international policy development and execution.

c. Defense Information Systems Network (DISN) – Enterprise Activities: Defense Information System Network (DISN) is the DoD's consolidated worldwide telecommunications infrastructure that provides end-to-end information transport for DoD operations, providing the warfighters and the COCOMS with a robust C4I information long-haul transport infrastructure. The DISN goal remains to seamlessly span the terrestrial and space strategic domains, 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 wide-bandwidth that is populated with the information and information services that our forces need."

The primary focus in FY 2009 continues to be the transition of Access Transition Initiative (ATI) circuits from expiring contracts to either the new DISN Access Transport Services (DATS) contracts or onto the DISN Core. This is a multi-year activity that consumes $25.2 million or 46 percent of the annual funding in FY 2009. The non-recurring

I. Description of Operations Financed: (continued)

transition costs include planning and integration, contractor labor, minor equipment, installation, circuit dual operations, travel, and testing to ensure uninterrupted customer service. In addition, recurring Operation and Maintenance costs for DISN bandwidth in Kosovo, Defense Satellite Communications System (DSCS), and Enhanced Pentagon Capability (EPC)/Survivable Emergency Conferencing Network (SECN) are estimated at $16.4 million or 30 percent of the annual funding. Kosovo funds reimburse circuit costs incurred in the Defense Working Capital Fund. The DSCS and EPC/SECN costs are comprised of technical assistance, depot support, maintenance, licenses, program support, and circuit engineering. Lastly, the remaining FY 2009 funding is for pay, benefits, and program support for DSCS and Senior National Military Command System plus management support activities which include quality assurance, logistics, and applications sustainment. $1 million is planned in FY 2008 and FY 2009 to support operational requirements associated with **Internet Protocol version 6 (IPv6).**

The DoD has designated the DISA as the only authorized provider of commercially leased Satellite Communications (SATCOM) services and the Systems Engineer for Satellite Communications (SES). The DISA is implementing a capabilities-based, best practice strategy that provides more responsive, customer-focused, and cost effective COMSATCOM services for the Warfighter. The DISA will enhance the operational effectiveness and efficiency of its primary commercial satellite contracts (i.e., DSTS-G and Inmarsat), reduce the service provisioning process time, improve performance management, improve overall customer satisfaction and quality of service and develop the future services acquisition approach to support the long-term joint war-fighting Commercial SATCOM Communications services requirements. As the DISA’s organization of record, the SATCOM Program Management Office (SATCOM PMO) needs appropriate funding to properly execute this mission on behalf of Congress and the DoD. The SES develops from mid and long-term overarching SATCOM architectural recommendations specific “system of systems” concepts

I. Description of Operations Financed: (continued)

and recommendations for the midterm that can be turned into and/or mapped to specific requirements and capabilities documents for SATCOM systems as directed by the Joint Requirements Oversight Council (JROC). These systems will then be developed, acquired and fielded by the appropriate acquisition activity, with technical support and guidance from USSTRATCOM and designated SSEs to ensure seamless integration and operation with other SATCOM capabilities and the overarching GIG. The SES collaborates with the EA for Space, Services, USSTRATCOM, SSEs and program offices in the area of architectural roadmap and engineering during the design and development of SATCOM systems to ensure interoperability and compliance with SATCOM system standards. The SES performs engineering analyses and other studies of system performance as requested by OASD(NII), Joint Staff, MCEB and USSTRATCOM. The SES assists USSTRATCOM and the SSEs with terminal certification and waivers for their assigned systems. Perform technical evaluation to ensure all SATCOM systems and terminals are compliant with approved DoD SATCOM MILSTDs and agreements.

Defense Information Systems Network (DISN) Subscription: The Department has designated the DISA as the Systems Engineer for Satellite Communications (SES) and the only authorized provider of commercially leased SATCOM services. This role requires the DISA to develop and implement a more strategic approach for acquiring commercial satellite communications services. The SES develops from mid- and long-term overarching SATCOM architectural recommendations specific “system of systems” concepts and recommendations for the midterm that can be turned into and/or mapped to specific requirements and capabilities documents for SATCOM systems as directed by the Joint Requirements Oversight Council (JROC). These systems will then be developed, acquired and fielded by the appropriate acquisition activity, with technical support and guidance from USSTRATCOM and designated SSEs to ensure seamless integration and operation with other SATCOM capabilities and the overarching GIG. The SES collaborates with the Executive Agent for

I. Description of Operations Financed: (continued)

Space, Services, USSTRATCOM, SSEs and program offices in the area of architectural roadmap and engineering during the design and development of SATCOM systems to ensure interoperability and compliance with SATCOM system standards. The SES Performs engineering analyses and other studies of system performance as requested by OASD (NII), Joint Staff, MCEB and USSTRATCOM. The SES assists USSTRATCOM and the SSEs with terminal certification and waivers for their assigned systems, and performs technical evaluations to ensure all SATCOM systems and terminals are compliant with approved DoD SATCOM MILSTDs and agreements.

3. **Global Information Grid (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.

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 (IA) program reflects increases in FY 2009 as a result 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, DW account to the O&M, DW consistent with the Expense Investment criteria ($250 thousand 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)

Mission Area Component ($ in Thousands)	FY 2007	FY 2008	FY 2009
a. Network Operations	12,443	6,855	17,214
b. Info Systems Security Program/Info Assurance/PKI	247,577	247,683	316,562
c. Comprehensive National Cybersecurity Initiative			36,000
d. Field Commands and Field Offices	65,529	45,767	47,178
e. Joint Staff Support Center	6,270	23,281	24,399
f. Defense Industrial Base			2,000
GIG Network Operations and Defense Total	**331,819**	**323,586**	**443,353**

a. Network Operations (NetOps): NetOps provides the integration and synchronization of the Agency's many Theater NetOps Center (TNC)/ COCOM Network Operations & Security Capabilities (CNOSC) transformation initiatives to ensure timely capabilities improvements, improved efficiencies and business practices, end-to-end interoperability and reliable/secure operations. Key actions include:

- Integrate and synchronize GIG NetOps transformation initiatives focused on TNC enablers that provide improved effectiveness and efficiencies internally and vertically (GNC and Service NOCs), as well as emerging peers (non-DoD).
- Transformation planning and synchronized/integrated implementation of GIG NetOps in a real-time current operations and legacy systems environment.
- From cradle to grave, facilitate configuration control and requirements validation of uniform net-centric Global NetOps solutions; and, coordinate development of improved TTP and integration of technology. Ensure the transition and end-state implementation plans are properly tailored and synchronized for the Combatant Commander.

I. Description of Operations Financed: (continued)

The Global NetOps Center coordinates the DISA and JTF-GNO response actions to IA events across Service and Agency CERTS, appropriate federal and the DoD agencies, and Law Enforcement entities.

- Provides operational direction and control to, and maintains status of, the National Communications System (NCS) and the GIG. Directs multi-service military and civilian personnel accomplishing network management, analysis, and contingency operations.
- Performs and validates analysis of Computer Network Defense (CND) incidents. Performs containment, response, and restoral actions to maintain integrity of the GIG.
- Exercises operational direction of the Defense Satellite Communication System (DSCS) earth terminals and space segments through the DISA Area Communications Centers, the DSCS Operations Center and the Consolidated Space Test Center. Operates DSCS Operational Support Systems utilizing the DSCS Network Planning System to support critical warfighter operations.

The JTF-GNO Net Defense Team (CERT) protects, defends, and restores the integrity and availability of the essential elements and applications of the GIG under the full spectrum of conflict in support of the “Warfighter”.

- DoD’s primary technical point of contact for computer network defense and information assurance.
- Identifies and resolves computer security anomalies that affect the GIG’s ability to support SECDEF elements, Joint Staff, Supported COCOMS, and the warfighter.

I. Description of Operations Financed: (continued)

The Theater NetOps Center-Net Defense Branch (TNC-ND) supports full operations at CONUS, Pacific, Europe, & Central on a 24x7 basis.

- Provides a critical view of their respective AORs to their DoD customers. This view is uniquely interagency and GIG wide.

The Computer Emergency Response Team Coordination Center (CERT/CC) is part of the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU). The SEI is a Federally Funded Research and Development Center and Research Laboratory (FFRDC) sponsored by the Department of Defense (OUSD/ATL) and operated by Carnegie Mellon.

- Provides DoD, civil government, industry, and the private sector community coordination and technical support in detecting and resolving computer security incidents as well as taking steps to prevent future incidents from occurring.
- Provides the technical leadership to advance the practice of software engineering, allowing the DoD to acquire and sustain its software-intensive systems with predictable and improved cost, schedule, and quality.

Computer Network Defense Service Provider (CNDS) under this DoD initiative the DISA serves as the designated Certification Authority (CA) for DoD GENSER CNDS Providers. DISA supports this effort by deploying teams of functional experts tasked to conduct periodic on-site Certification and Accreditation (C&A) assessments. Evaluation teams are deployed globally to conduct performance and capability assessments of the CNDS Providers.

- Conducts comprehensive evaluations of the performance and capabilities of CNDS providers.
- Provides the guidance and assistance to improve the rating of poorly performing providers.

I. Description of Operations Financed: (continued)

The Combatant Commander Network Operations & Security Capabilities (CNOSC) provides operational, procedural and technological support to the Combatant Commander that allows him to effectively execute NetOps.

The CNOSC extends DISN services and support by delivering an integrated, end-to-end global awareness of NetOps within the Combatant Commander's GIG AOR. The Combatant Commander's GIG AOR includes the total end-to-end connectivity, both wired and wireless, that delivers voice, data, and video between the Combatant Commander and the assigned forces, components, groups and other organizations supporting the command's mission. By contributing to development of a situational awareness picture that includes all elements of the GIG, the CNOSC provides consistent, high quality DISN status information and directly supports the Combatant Commander's daily operational decision-making process.

The Joint Web Risk Assessment Cell (JWRAC) is a DEPSECDEF chartered cell within DISA responsible for conducting analyses of content and data resident on publicly accessible DoD Web sites.

- Sites are reviewed for compliance with existing DoD Web Policy and guidelines; remediation action is taken to bring a site in compliance.
- Performs analyses of the aggregate data to determine if an OPSEC risk exists that may pose an immediate or potential threat to the warfighter.

Sensor Grid Operations supports a defense-in-depth approach to Information Assurance (IA) by operating and managing Intrusion Detection Systems (IDS), Anomaly Detection Systems and Security Information Correlation.

- Provides IA protection at the perimeter, enclave, hub, and core levels of the GIG, allowing for an integrated view of all DoD Enterprise sensors.

I. Description of Operations Financed: (continued)

- Supports health, welfare, software development and configuration management for current systems and emerging IA requirement to expand current capabilities, address user defined requirements, and/or correct IA vulnerabilities.
- Responsible for the development, testing, and dissemination of Intrusion Detection Signatures that detect newly identified vulnerabilities on the GIG.
- Responsible for the piloting, lab tested IA hardware and software solutions to increase monitoring capabilities, reduce and correlate data traffic, and detect newly identified vulnerabilities on the GIG.

NetOps system integration support:

- Integrates, customizes, and implements COTS hardware and software, hardware and software license maintenance, and technical support for four operational sites.
- Operates, sustains, and secures the DISA's NetOps Common Operational Picture (DISA NETCOP) systems at all fielded sites.
- Accomplishes spiral development, providing enhanced capabilities of system baseline, as well as broadening the scope of the system to provide GIG NetOps situational awareness by integrating more NetOps data sources from COCOMS, Services, and Agencies.

b. Information Systems Security Program (ISSP)/Information Assurance (IA)/PKI:
The DISA ISSP refocused its IA efforts by taking a net-centric approach to addressing the Department of Defense's (DoD's) security demands on an enterprise wide scale. Moving toward a Common Services and shared information model requires networks to be more transparent and allow users seamless access to everything they need to focus on their mission rather than Information Technology (IT) administration. This approach requires

I. Description of Operations Financed: (continued)

some major adjustments to how IA will be integrated into this new architecture while focusing on designing and deploying proactive protections, deploying attack detection, and on performing IA operations to ensure that adequate security is provided for information collected, processed, transmitted, and disseminated on the GIG. To rapidly achieve this new vision for defending the GIG, the DISA will: identify threats facing existing networks, codify the implementation strategy, align the program with priorities, and evolve to serve as a component of the larger NetOps solution.

The ISSP will purchase enterprise licenses to maintain Computer Network Defense (CND) tools and contractor support that develop, test, help field, operate and sustain IA capabilities. 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 customers with the ability to maintain information superiority in all environments.

The DISA and the JTF-GNO will provide support to the Federal Government’s response to the cyber security threat.

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 all information maintains a level of trust commensurate with mission needs. DISA accomplishes this goal in FY 2008 and FY 2009 by:

- Providing up-to-date anti-virus and anti-spyware tools to protect computer hosts from compromise, detect and clean infected systems, and prevent further contamination from

I. Description of Operations Financed: (continued)

those threats for approximately 4-million DoD enterprise and Coast Guard owned and controlled desktops, laptops, personal electronic devices, servers, and email & web applications.

- Operating and sustaining the Joint Enterprise Directory Service (JEDS) harvesting and publishing service used to develop DoD White pages, allow search capability, and support GIG attribute based access control data authorization methodologies, enabling truly secure Net-Centric Enterprise Services for the Intelligence Communities (IC), allies, and coalition partners.
- Providing enterprise-wide unlimited DoD licenses for directory server, web server products, and client/server digital certificate licenses which support the issuance of over 12 million identities.
- Operating and Sustaining the Global Directory Services (GDS) enabling reliable sharing of certificate revocation lists and individual's Public Keys across the DoD.
- Operating and Sustaining initial Authentication and Privilege Management capabilities being developed by NSA that will enable authorization decisions built upon access control methodologies to ensure any data existing within the enterprise about a user, a situation, or a transaction is available beginning with initial capability in FY 2008 and additional deployments and operational sustainment in FY 2009.
- Providing enterprise-wide tools and engineering, networking, and architecture support to detect, locate, and mitigate wireless threats in both fixed and mobile environments.

DISA DEFENDS SYSTEMS AND NETWORKS to ensure no access is uncontrolled and all systems and networks are capable of self-defense by "building in" technologies recognizing, reacting, and responding 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 and

I. Description of Operations Financed: (continued)

threats posed by the insider, 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 all information systems that traverse a DoD enclave boundary are secure. The DISA's efforts under this goal encompass:

- Sustaining subnets called DeMilitarized Zones (DMZs) that sit between trusted internal networks and untrusted external networks that protect the DoD infrastructure by simultaneously improving the ability for authorized users to access shared data while keeping them away from unshared data during FY 2008 – FY 2009.
- Installing and maintaining firewalls for the SIPRNet GIG Transport network and COCOMS/Services/Agencies premise/enclaves locations, and non-service SIPRNet access points and connections during FY 2008 – FY 2009.
- Providing comprehensive and robust security examinations of SIPRNet and NIPRNet sites identified by the Joint Task Force – Global Network Operations (JTF-GNO) to ensure compliance with security policies and identify common vulnerabilities across the GIG during FY 2008 – FY 2009.
- Fielding and maintaining intrusion prevention and content filtering tools that block known malicious inbound and outbound traffic at the boundary between the NIPRNet and Internet Gateway by observing, detecting, and reacting to attacks against the Internet Protocol (IP) based infrastructure and/or customers during FY 2008 – FY 2009.
- Providing an enterprise-wide Insider Threat Focused Observation Tool (InTFOT) used selectively deploy a host-based agent to analyze and characterize risks associated with a potential insider threat to information and information systems with fielding beginning FY 2008.

I. Description of Operations Financed: (continued)

- Providing an enterprise-wide Insider Threat Detect (InTDET) solution to detect and alert on potential insider threat activities. An "insider" is anyone who uses authorized credentials to access a DoD system. Fielding in FY 2009.
- Developing an automated Network Access Controls (NAC) for the SIPRNet to ensure consistent access across the enterprise with deployment beginning FY 2009.
- Publishing Security Technical Implementation Guidance (STIGs) via industry data standards that allow the description of vulnerabilities and compliance checks in terms that can be directly consumed by commercial tools FY 2008 – FY 2009. The ultimate goal of this data standards effort is to become vendor agnostic while sharing information between policy creators, tools, tracking systems and visualization systems such as the UDOP.
- Providing the DoD GIG Common Operational Picture (COP) SA tool to demonstrate the technical challenges of integrating disparate data from stove-piped NetOps source systems across the enterprise and correlating with other data to determine root cause analysis and present the information in cogent displays (dashboards) for the JTF-GNO and TNCs during FY 2008 – FY 2009.
- Supporting the Certification and Accreditation (C&A) activities through an automated system that provides a security profile containing situational awareness of registered information systems for analysts and reduces the amount of time and cost to certify and accredit systems during FY 2008 – FY 2009.
- Providing Senior DoD Officials, the Intelligence Communities (IC), and network administrators vulnerability information, compliance guidance and a centralized registry of DoD users AISs ports and protocols which they use to enable interoperability while simultaneously restricting unauthorized access to those systems during FY 2008 – FY 2009.

I. Description of Operations Financed: (continued)

- Providing a Secure Compliance Remediation Initiative (SCRI) enterprise tool that automatically feeds asset level information to the Vulnerability Management System (VMS) and protects systems identified in the Vulnerability Compliance Tracking System (VCTS) by automatically correcting vulnerabilities and isolating the devices from the network until remediation occurs bringing the system into compliance with the latest vulnerability patches during FY 2008 – FY 2009. Developing SCRI capabilities to support the publication of asset, vulnerabilities and assessment data using Computer Network Defense (CND) data schemas and Security Content Automation Protocol (SCAP) standards during FY 2008 – FY 2009.
- Fielding and maintaining Intrusion Detection Systems (IDSs) that detect attacks, characterize the type of attack, offer limited responses to the attack, and identify suspicious activity via signature matching for the Theater Network Center (TNC) and JTF-GNO during FY 2008 - FY 2009.
- Operating a secure, accurate and accessible Domain Name Service (DNS) to protect the DoD infrastructure from security vulnerabilities such as DNS cache poisoning, denial of service, corrupted databases and compromised servers during FY 2008 - FY 2009.
- Supporting the development of Concept of Operations (CONOPS) documentation and providing laboratory services (develop test plans, evaluate candidate products, perform security and functional testing) in support of source selection activities that provide DoD-wide capabilities during FY 2008 - FY 2009.
- Providing the Gold Disk enterprise-wide tool used to configure systems by automatically setting permissions, making registry changes, installing patches, and disabling unneeded services during FY 2008 - FY 2009.
- Operating and maintaining the DoD Patch Management System enterprise-wide tool used to distribute and install vendor patches, tools and updates during FY 2008 - FY 2009.

I. Description of Operations Financed: (continued)

- Assisting the JTF-GNO by providing tools to identify the architecture and perimeter of the GIG, particularly providing the ability to map the backbone of the SIPRNet (identifying all wired and wireless access points and detecting leaks to other networks) and the NIPRNet (identifying all enclave connections and detecting all Internet and unauthorized connections) during FY 2008 - FY 2009.
- Bundling the data from multiple web applications into the System/Network Approval Process (SNAP) database enabling DoD to collect, track and report IT accreditation and IA security posture standing as required by DoD policy for all unclassified DISN data connections at the base, installation, post, station and facility during FY 2008 - FY 2009.
- Maintaining a web portal and robust database used to document and track Connection Approval Process (CAP) information and maintaining a CDS registry for the SIPRNet and classified DMZs during FY 2008 - FY 2009.
- Providing technical and administrative expertise in support of the accreditation of DoD Information Systems to maintain a favorable accreditation status for over 122 mission critical systems registered in the DoD IT Registry, the DoD IT Portfolio Registry (DITPR) and over 400 internal support systems during FY 2008 - FY 2009.
- Providing analytical, technical, administrative, and logistical support to the Defense IA Security Accreditation Working Group (DSAWG) which serves as a community forum for reviewing and resolving authorization and connection decisions related to the sharing of information about IA and security risks, advises the DISN/GIG Flag Panel, the DoD Senior IA Officer (SIAO), and affected DAAs on authorization and connection decisions, and interacts with the DIACAP Technical Advisory Group (TAG) to examine C&A issues and improve DoD IA C&A Process Guidance (DIACAP) Knowledge Service (KS) content during FY 2008 - FY 2009.

I. Description of Operations Financed: (continued)

DISA PROVIDES INTEGRATED IA SITUATIONAL AWARENESS (SA) AND IA COMMAND AND CONTROL (C2) by giving decision makers and network operators at all command levels the tools for conducting IA and CND operations in Net-Centric Warfare (NCW). To further this goal, DISA is:

- Developing enterprise acquisition and implementation plans to support the enterprise-wide deployment of sensors, and sustaining already existing systems, which support the correlation and analysis of CND events and activities looking for intrusions and anomalies at the enclave, network and host levels, and mitigating and responding to attacks directed at the GIG beginning with deployment in FY2008.
- Sustaining the Host based Security System (HBSS) automated and standardized tool on both the SIPRNet and NIPRNet to provide end-point security against both insider and external threats able to penetrate boundary defenses or enter through backdoors during FY 2008 - FY 2009.
- Providing enterprise-wide tools for collecting, storing, retrieving and analyzing header flow data and metadata from border routers on the NIPRNet and the backbone routers on both the NIPRNet and SIPRNet during FY 2008 - FY 2009.
- Developing, deploying a User Defined Operational Picture (UDOP) capability to share integrated Situational Awareness (SA) data allowing analysts, watch officers, and commanders to collaborate and formulate courses of action and evaluate resultant impact on local, intermediate, and DoD-wide CND activities and operations during FY 2008 - FY 2009.
- Developing Technical Media Analysis Tools (TMAT) to provide the capability to trace cyber attacks to their sources and accurately identify and characterize the attacking activity information warfare capabilities with initial deployment in FY 2008.

I. Description of Operations Financed: (continued)

- Providing technical management and assistance, development oversight, and maintenance for the Joint Computer Emergency Response Team (CERT) Database (JCD) suite of computer incident reporting and tracking databases allowing JTF-GNO analysts across the enterprise to share data and resources ensuring rapid and secure retrieval of information supporting decisions during FY 2008 - FY 2009.
- Maintaining the DoD CERT Incident Database (DCID) used to collect CERT related incident handling and reaction data from the Regional TNCs and other DoD customers, and then feed this information to the JCD and Trouble Management System (TMS) during FY 2008 - FY 2009.
- Maintaining the Joint Threat Incident Database (JTID) used by Intelligence Communities (IC) analysts to correlate threat and hacker data with specific incidents to develop and analyze problem sets and then make long and short-range predictions of threat intentions and capabilities during FY 2008 - FY 2009.

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

- Providing an IA Portal on the Defense Knowledge Online (DKO) for disseminating IA documents, related links, resources and additional support across the enterprise.
- Collaborating with the National Security Agency (NSA) to provide an opportunity for the DoD IA community to identify and resolve IA issues, develop strategies, and demonstrate new IA technologies.

I. Description of Operations Financed: (continued)

DISA CREATES AN IA EMPOWERED WORKFORCE well equipped to support the changing demands of the IA environment by establishing baseline certifications across the enterprise-wide architecture, 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. 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.
- Providing mission related private sector training and conferences for government employees.
- Designing and delivering hands-on IA classroom training to security professionals, system and network administrators, and system users throughout the joint community.

The Department of Defense (DoD) Public Key Infrastructure (PKI) is the mechanism that provides public key certificates to support mission critical DoD applications, and provides the Department's information assurance (IA) needs for confidentiality and authentication of network transactions, identification and verification of data integrity, and non-repudiation of communications or transactions as well as digital signature. The DoD PKI is available on both the NIPRNet and SIPRNet. PKI must evolve to accommodate Homeland Security Presidential Directive –12 (HSPD-12).

The National Security Agency (NSA) is the DoD PKI Program Manager, and as such they provide funds for the engineering support for new capabilities for the DoD PKI. All other functions and activities for the DoD PKI are conducted and funded by DISA as the Deputy Program Manager, through the Information Assurance Program. This includes, but is not limited to system upgrades, implementation, operation, and sustainment; PKI

I. Description of Operations Financed: (continued)

registration authorities training; and JITC interoperability testing, procurement of equipment, software and hardware acquisition and maintenance.

c. Comprehensive National Cybersecurity Initiative: The Department will play a critical role in this initiative by enhancing the security of Defense networks and the protection of Defense information.

d. Field Commands and Field Offices: The DISA's three Field Commands and seven Field Offices are forward deployed and co-located with the Combatant Commands (USJFCOM, USTRANSCOM, USSOUTHCOM, USSTRATCOM, USSOCOM, USCENTCOM, USNORTHCOM, USEUCOM, USPACOM).

The DISA Field Commands and Offices serve as a liaison between DISA and the Combatant Commanders/Component Commanders on DISA support issues and policies. The Field Offices ensure that issues identified by Commanders are resolved in a time-sensitive manner and function as the focal point within DISA for theater-unique requirements. They maintain a proactive role with other Field Office/Commands and Combatant Commander representatives, managing requirements from identification to delivery of DISA services. In addition, DISA's Continental U.S. Global Network Support Center (GNSC) exercises centralized management of CONUS network operations and are responsible for the real-time operational direction, monitoring and control of the DISN networks within CONUS.

e. Joint Staff Support Center: The JSSC provides information technology and command and control (C2) support that enables the Joint Staff (JS) to perform its mission of supporting the warfighter. JSSC conducts 24x7 watch/monitor operations in the National Military Command Center (NMCC) for Command, Control, Communications, Computers, and Intelligence (C4I) systems, strategic threat operational warning, and local Global Command and Control System (GCCS) - Joint operations maintenance. The JSSC provides the

I. Description of Operations Financed: (continued)

JS with software-applications support relating to operational capabilities in conventional and nuclear planning and operations. JSSC provides studio and remote video and audio recordings, electronic graphics, post production editing for Defense-wide training, informational, gun camera and battle damage assessment assistance, and guidance for video teleconferencing networks and operations. The 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. The FY 2008 to 2009 increase supports the lifecycle management of the GCCS-J architecture supporting the NMCC.

4. Exploit the GIG for Improved Decision Making: This mission area funds key C2 activities including the GCCS-J; the GCSS, NMCS; Defense Message System (DMS); and Net-Enabled Command Capability. The GCCS Family of Systems programs deliver C2 capabilities specified in their respective requirements documents, and plan to transition GCCS to a joint, net-centric C2 capability. The DISA has 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.

I. Description of Operations Financed: (continued)

Mission Area Component ($ in Thousands)	FY 2007	FY 2008	FY 2009
a. Global Command and Control System-Joint	104,100	76,183	89,247
b. Global Combat Support System	13,544	15,694	17,832
c. National Military Command System	18,271	6,507	6,935
d. Defense Message System	19,533	12,924	16,176
e. Combined Enterprise Regional Information Exchange System	14,665	25,179	40,373
f. Net-Enabled Command Capability	11,044	9,730	35,717
g. Electronic Commerce	145	0	13,790
h. Other Programs	16,421	13,155	13,279
Exploit the GIG for Improved Decision Making Total	**197,723**	**159,372**	**233,349**

a. Global Command and Control System-Joint (GCCS-J):
The GCCS-J is the DoD joint 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. The GCCS-J provides a robust and seamless C2 capability to the Commander-in-Chief, Secretary of Defense, NMCC, COCOMS, Joint Force Commanders, and Service Component Commanders. Employing the DISN, GCCS-J offers vital connectivity to the systems the joint war fighter uses to plan, execute, and manage military operations. The GCCS-J is a major IT 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

I. Description of Operations Financed: (continued)

specific set of Joint Staff validated and prioritized user requirements, and delivers multiple releases of GCCS-J functional capabilities. The 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 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.

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

The GCCS-J is responsible for the sustainment of the Common Operating Environment (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.

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 deliberate planning timeline from two years to six months. The CFAST facilitates the dynamic preparation of campaign plans for rapid expeditionary

I. Description of Operations Financed: (continued)

environments to meet DoD planning doctrine requirements of ongoing operations such as the Global War on Terrorism (GWOT) and future contingencies.

In FY 2009, these activities sustain the GCCS-J Block V version releases (GCCS-J v4.1 and GCCS-J v4.2) and will begin the migration of the JSSC to the DISA Defense Enterprise Computing Centers (DECC) to support net-centric operations. These activities will correct deficiencies and problem reports, and maintain the security posture of the GCCS-J system as new threats and vulnerabilities are identified. GCCS-J will be sustained until such time as NECC's capabilities are available for use.

b. Global Combat Support System (GCSS)

The GCSS(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. The GCSS provides the CC/JTF commanders with fused CS data and C2 information on the same workstation. The GCSS (CC/JTF) provides the information technology (IT) capabilities required to move and sustain joint forces throughout the spectrum of military operations.

Per direction of the Joint Staff (JS), within the GCSS Family of Systems (FoS), DISA is responsible for two main efforts: system architecture and engineering for the GCSS FoS, and development, integration, fielding, operation and maintenance of the GCSS (CC/JTF). The GCSS (CC/JTF) provides enhanced CS situational awareness to the joint war fighter 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. For FY 2008 through

I. Description of Operations Financed: (continued)

FY 2009, the program is incrementally implementing a service-oriented architecture (SOA) in a net-centric environment utilizing the Net-Centric Enterprise Services (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), Contingeny Site, Enterprise System Management (ESM), and security (e.g., intrusion detection on GCSS strategic servers and next generation guards) processes and tools. This new architecture enables the program to become fully net-centric and enables accelerated introduction of new data source integration and application development; permits greater flexibility for the end-user in how they evaluate and view fused data; increases dynamic report capability; provides more rapid exposure of data to communities of interest; and increases security.

In FY 2008 – FY 2009, GCSS (CC/JTF) continues to maintain and support fielded capabilities at the Combatant Commands and supporting Component Headquarters. This includes delivering system upgrades in the form of major software releases, and updated/rapid fixes in support of prioritized Combatant Command requirements to support day-to-day combat operations. In addition, these activities include Enterprise Systems Management and problem resolution support, and hardware/software license and maintenance costs. Improved COOP, Contingency Site, and security enhancements are included (e.g., intrusion detection, next generation guards). Training and onsite functional and technical support at the Combatant Commands are provided to users with new capability increments by GCSS (CC/JTF), and supports exercises and demonstrations as directed by the JS J4. Operational security of the systems (i.e., managing and implementing security patches in response to Information Assurance Vulnerability Alerts, supporting Security Test & Evaluations of the system to maintain our Authority to Operate, and supporting

I. Description of Operations Financed: (continued)

Security Readiness Reviews) at our operating locations is maintained through this activity.

c. National Military Command System (NMCS):
The NMCS provides Senior Leaders; National Military Command Centers (NMCCs); 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 command and control (C2) capabilities, ensure continuous availability of emergency messaging, and maintainsituational and operational awareness. The DISA 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, situational 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 Agency's mission 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 COCOMS.

The FY 2008 through FY 2009 program includes enhanced capabilities for performing configuration management of NMCS assets (particularly C2 systems) and facilities; providing technical assessments and engineering support to modernize the NMCS via technology insertions; implementation of an Information Resources Management (IRM) infrastructure; mirroring of NMCC systems at the alternate NMCC via the Site R Integration Program.

I. Description of Operations Financed: (continued)

Additionally, FY 2009 funding supports NMCS/NCCC 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. Defense Message System (DMS):
The Defense Message System (DMS) is the official DoD Warfighter Message System that meets/exceeds Joint Staff criteria for providing secure, timely, reliable and accountable organizational messaging and associated directory services. The DMS is the integrated writer-reader capable system, globally accessible by strategic/tactical sites, as well as interfaces with our Allies, non-DoD agencies, and Defense contractors. The DMS utilizes COTS and modified COTS components to provide multi-media messaging and directory capabilities that complement and leverage the GIG. In May 2005, ASD/NII placed DMS in sustainment through 2012. Sustainment allows minor system/product adjustments, bug fixes, and operational/integration testing to correct security shortfalls and maintain the objective system.

This activity supports the global DMS community's (Services/agencies/COCOMS) operational, sustainment system engineering and sustainment integration activities; program cost analysis; and milestone management, as overseen by the DMS Global Service Manager.

I. Description of Operations Financed: (continued)

e. 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). The CENTRIXS supports intelligence and classified operations; information exchange and sharing at the classified 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 GWOT. These networks allow the United States to share information rapidly with coalition partners worldwide in support of local, regional, and global combined operations. The CENTRIXS architecture is both network-centric and web-centric, using a combination of readily available COTS and GOTS solutions to reduce implementation costs while providing a robust, innovative approach to warfighting communications. The 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 plus NATO, 11 Bilaterals and 150 sites worldwide. Currently, it has 26,000 users and the user community continues to grow. 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.” In FY 2008 and beyond, funding will sustain the CENTRIXS-enhanced footprint and enable continued coalition information sharing in support of the aforementioned multinational efforts.

I. Description of Operations Financed: (continued)

Operational support to CENTRIXS includes procurement, logistics, training, and, associated technical/engineering expertise necessary to maintain and sustain these systems. Funds will be used to complete the centralization of service hosting and convergence of CENTRIXS and Griffin capabilities into a single capability allowing approved interaction between national Classified 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. The CENTRIXS Cross Enclave Requirement (CCER) effort will satisfy COCOM coalition information sharing requirements without Cross Domain Solution (CDS). It will converge various CENTRIXS networks into a single warfighting information sharing environment.

f. Net-Enabled Command Capability (NECC)

The Net-Enabled Command Capability (NECC) is the DoD's principal command and control capability that will be accessible in a net-centric environment and focused on providing the commander with the data and information needed to make timely, effective and informed decisions. NECC draws from the command and control (C2) community to evolve current and provide new C2 capabilities into a fully integrated, interoperable, collaborative joint solution. Warfighters can rapidly adapt to changing mission needs by defining and tailoring their information environment and drawing on capabilities that enable the efficient, timely and effective command of forces and control of engagements.

The DoD has placed its emphasis upon NECC as the future of C2 for the Warfighter. The Department cannot accomplish its mission to provide an integrated flexible, and adaptable full spectrum DoD C2 capability by continuing to rely on independently built and deployed systems that result in variations in situational awareness and force identification, data

I. Description of Operations Financed: (continued)

incompatibilities, and non-interoperable services and applications for time-critical decisions. Consequently, the Deputy Secretary of Defense directed that DoD funding be internally realigned into the NECC Program. These funding realignments provide for a single, integrated, coherent enhancement of the Department's capability for operational level C2.

In FY 2009, the program will begin replacing the current C2 stovepiped capabilities, represented by the Global Command and Control System Family of Systems (GCCS FoS). Those GCCS FoS applications supporting the envisioned NECC concepts will evolve from their current state of joint and Service variants into a single integrated capabilities-based, NECC architecture. The NECC will provide the capability to collaboratively plan execute, monitor, and assess joint and multinational operations by enabling vertical/horizontal information exchange across the joint/coalition command and control community. In addition to achieving interoperatiblity across the mission space, NECC will facilitate the exchange of information across multiple security domains and will reduce logistics/support requirements.

5. Deliver Capabilities Effectively/Efficiently: This mission area funds the DISA Management Headquarters activities, payments levied to fund the costs that 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.

The 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, DISA established a methodology for consistently assigning shared costs across programs

I. Description of Operations Financed: (continued)

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, operating costs of 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 DISA's internal LANs, WANs, and IT services.

Implementing this initiative significantly improves 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 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.

I. Description of Operations Financed: (continued)

Mission Area Component ($ in Thousands)	FY 2007	FY 2008	FY 2009
a. Management Headquarters	27,318	34,131	35,301
b. Pentagon Reservation Maintenance Revolving Fund	14,575	14,142	14,998
c. Shared Service Units	47,315	15,086	18,112
d. Other Programs	20,517	50	55
Deliver Capabilities Effectively/Efficiently and Shared Services Total	**109,725**	**63,409**	**68,466**

a. Management Headquarters

Management Headquarters is responsible for overseeing, directing, and controlling DISA activities. DISA activities include both those funded with appropriated funds and Defense Working Capital Funds (DWCF). The Management Headquarters staff provides the leadership for implementing DISA's Transformation Roadmap 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 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 DISA and supportive of Global Net-Centric solutions. Management Headquarters accounts for Agency-wide

I. Description of Operations Financed: (continued)

congressionally mandated functions, such as the Equal Employment Opportunity Office and the Inspector General.

One of the challenges Management Headquarters is facing at DISA is a personnel imbalance in skills mix at a time when overall attrition is declining. This imbalance needs to be monitored and controlled as the agency moves forward with implementation of the FY 2005 Base Realignment and Closure Act and the relocation to Ft. Meade, MD. To help correct this imbalance in skills mix and ensure the agency has key skill sets necessary to support the mission, the agency is offering voluntary separation incentives in FY 2008 to voluntarily separate personnel where skills are no longer required or are required at a reduced rate. Examples are more evident where systems are migrating from development to that of an implementation and sustainment mode. All new and increased skills are required to support missions transferring into the agency in FY 2008 and FY 2009, and in areas where the agency has high turnover in critical skills areas, such as procurement, budget, engineering, etc. The FY 2008 and FY 2009 budget estimates support the agency's Human Capital Plan which provides for the overwhelming majority of the jobs voluntarily separated in FY 2008 to be reengineered with new interns of the right skills mix. It allows the agency to hire highly qualified experts consistent with approved OPM and DoD policy, as well as offer incentives and retention bonuses to hire and retain personnel with key skills, such as engineers, contracting officers, contracting specialists, budget analysts, etc.

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

I. Description of Operations Financed: (continued)

provides the framework for DISA organizations to develop their appropriate level goals, 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 DISA's customers to ensure that 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 DISA receives. The challenges addressed by the Agency senior leaders revolve around the achievement of 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.

FY 2009 funds will provide for a safe, secure, healthy, energy-efficient, and high quality work environment so that DISA employees can perform their jobs effectively and efficiently. Funds will support rent costs normally incurred in a year as well as the following areas of operation:

I. Description of Operations Financed: (continued)

(1) Tenant charges and real property operations for Site R which is the alternate command and control location and capability for the Department of Defense if the Pentagon is attacked or unable to carry out all functions.
(2) Redundant voice, messaging and data network pathways to support the Virtual Pentagon, now called the Command Communications Survivability Program which fixes vulnerabilities in the command communications systems of Pentagon senior leaders.
(3) Pentagon Force Protection Agency (PFPA) support of PRMR.
(4) Information technology equipment to include wedge three network devices and swing space optical rings.

c. Shared Services Units (SSU)

The SSU resources are allocated across the products and services contained in the business and mission activities. The model which allocates the funds 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 (civilian, military, and contractor), and (4) amount of dollars in the business and mission projects.

- Chief Financial Executive (CFE) Office of the Chief Financial Executive (CFE) activities in the Mission Support area focus on the legislative mandates contained in the Chief Financial Officer (CFO) Act and the Government Performance and Results Act (GPRA) as well as the Budget and Performance Integration goal of the President's Management Agenda (PMA). The Directorate provides financial services support and financial automation support to the Agency as well as annual Agency-wide financial statements. They conduct economic analyses, cost estimating, and program and organizational assessments. A major challenge is to provide accurate, reliable,

I. Description of Operations Financed: (continued)

and timely financial information in a cost-effective way to support planning, engineering, acquiring, and fielding Global Net-centric solutions and operating the Global Information Grid. Continue implementation and contractor support in FY 2008 and FY 2009 for a clean financial audit opinion.

- Component Acquisition Executive (CAE) DISA has a dedicated Component Acquisition Executive (CAE) to focus exclusively on all acquisitions managed by DISA to include Major Automated Information Systems (MAIS), IT Services, Acquisition Category (ACAT) III programs, projects and services being acquired by DISA. The purpose of the CAE program activities is to provide acquisition leadership for the implementation of the net-centric vision through providing of tailored acquisition policies, processes, procedures, tools, lifecycle oversight and a qualified workforce that rapidly acquires quality products and services that satisfy user needs and provides measurable improvements to mission capabilities at a fair and reasonable cost.

  DISA's multi-tiered acquisition structure consists of the Office of the Component Acquisition Executive (CAE) and the four major portfolios with Program Executive Office (PEO) - like responsibilities. This portfolio-based structure is patterned after the PEO structures of the MILDEPs - a normalizing step DISA has taken along the maturity path of acquisition management within DISA. A criteria-based approach was used to determine portfolio content for each DISA acquisition, which included all programs, projects and the acquisition of services for which DISA is responsible. The four PEOs or major portfolios are Command and Control Capabilities, Information Assurance/NETOPS, GIG Enterprise Services and SATCOM, Teleport and Services. The leadership of these portfolios is provided through either a General Officer or member of the Senior Executive Services (SES). Specific contents of these portfolios will be addressed in other paragraphs.

I. Description of Operations Financed: (continued)

Several minor portfolios under the leadership of an SES have been established and generally contain ACAT III and below programs and service acquisitions. The DISA acquisition process is fully compliant with the DoD directives which defined the DoD Acquisition System, and includes working under appropriate OSD oversight while delivering joint capabilities to the warfighter.

- Manpower, Personnel and Security (MPS): The Manpower, Personnel and Security Directorate (MPS) develops and implements 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) The Procurement and Logistics Directorate (PLD) functionally transferred into the Defense Working Capital Fund (DWCF) in FY 2008.

- Strategic Planning and Information (SPI) The SPI supports the Director, DISA, in decision-making; strategy-development and communicating that strategy both internally and externally; aligning 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; and information assurance and management of DISA information technology resources. As a shared services unit, SPI supports 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 DISA and provides Agency oversight for IT systems. SPI serves as the

I. Description of Operations Financed: (continued)

Agency lead for performance and results-based management, budget and performance integration, strategy execution, and management of strategic customer requirements. SPI leads the Agency in developing its enterprise architecture and internal IT Enterprise applications; conducting IT capital investment planning; overseeing records management; and providing information assurance support to include the accreditation of the DISA information systems. SPI is 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 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 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 DISA employees and contractors in 35 locations worldwide (8 National Capital Region (NCR), 14 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 DISA internal/external customers including the Joint Staff.

The 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

I. Description of Operations Financed: (continued)

to validate methodology; assures data standardization, compliance, and interoperability of CIP IT Systems; and identifies GIG critical assets.

The SPI provides the DISA a world-wide Continuity of Operations (COOP) Program in accordance with DoD Directives and Executive Branch national guidance. Specifically, SPI maintains and improves the functionality of DISA relocation facilities; reviews, rewrites, staffs, publishes, and implements 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. This function will be transferred to the GIG Operations Directorate in FY2008.

The SPI manages 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." DISA's KM initiative will help generate, capture, integrate, and disseminate information and knowledge that is relevant to DISA's mission. The key technology supporting 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. Phase 3 is focused on deploying the EDGE Agency-wide in an unclassified environment, establishing a classified instance of

I. Description of Operations Financed: (continued)

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 integration of DISA's knowledge management capabilities with DoD-level knowledge and information sharing initiatives such as Defense Knowledge On-line (DKO), Net-centric Enterprise Services (NCES), and hosting at Defense Enterprise Computing Centers (DECCs).

Special Missions: In response to Executive Orders, Presidential Directives, DoD Directives, DISA provides engineering, information systems, communications, and operational support to the President as the Commander-in-Chief (CINC). These responsibilities were specified in the Defense Information Systems Agency's Charter - Department of Defense Directive 5105.19 - which tasked DISA to be "responsible for planning, developing, and supporting command, control, and communications (C3) that serve the needs of the President and the Secretary of Defense under all conditions of peace and war". Reliable, robust, and redundant communication and information systems are critical to positive control over U.S. Armed Forces. 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.

To support this mission, DISA has consolidated Presidential Support under Special Missions. 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 consist of several sub-activities: White House Communications Agency (WHCA), White House Situation Support

I. Description of Operations Financed: (continued)

Staff (WHSSS), White House Support, Senior Leadership Communications System (SLCS), Crisis Management System (CMS) (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 CINC communications across the range 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 2007	FY 2008	FY 2009
a. White House Communications Agency	98,961	119,325	130,194
b. White House Situation Support Staff	8,444	6,015	6,094
c. Crisis Management System	8,709	8,917	9,627
d. Minimum Essential Emergency Communications Network	7,986	7,687	7,891
e. Communications Management Control Activity	2,979	851	887
Special Mission Area Total	**127,079**	**142,795**	**154,693**

a. White House Communications Agency (WHCA)

WHCA is a joint service military agency under operational control of the White House Military Office (WHMO) and the administrative control of DISA. WHCA 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. WHCA's Operation and Maintenance appropriation provides funding to operate both the fixed and travel communications mission, such as:

I. Description of Operations Financed: (continued)

(1) Expanded support to the Office of the Vice President.
(2) White House Continuity of Government requirements.
(3) WHCA assumption of the audio visual mission, to provide audio visual and photographic services, in accordance with Public Law 109-163.
(4) Presidential and Vice Presidential trip support, that based on historical data is projected to increase to an average of 1,045 missions/year. The number of missions is projected to increase beyond the average of 1,045 during the 2008 presidential election year.
(5) Life cycle replacement, replenishment, technical refreshes, and sustainment costs related to maintaining continuity of Presidential and Vice Presidential communications.

The WHCA's budget provides communications support to the United States Secret Service (USSS). The Presidential Protection Assistance Act of 1976, Public Law 94-524, Section 6 and Defense Appropriations Act of 1997, Public Law 104-208, Title VIII, Section 8100 requires the Department of Defense and WHCA provide assistance on a temporary basis without reimbursement when assisting the Secret Service in its duties directly related to the protection of the President, the Vice President or other officer immediately next in order of succession to the office of the President. In accordance with these directives, WHCA provides fixed and mobile telecommunications support at the White House Security Complex in the Washington, D.C. Metropolitan Area and Camp David, Maryland, as well as on all trip sites both in and out of CONUS. In 2009, WHCA expects to expend approximately $7 million per year, in support of the USSS. The largest portions, approximately 75%, of the funds, are expended for the items provided to USSS on trip sites.

I. Description of Operations Financed: (continued)

b. White House Situation Support Staff (WHSSS)

The White House Situation Support Staff (WHSSS) was created by Presidential direction. WHSSS provides classified communications, computer, and intelligence systems for the National Security Advisor, White House Situation Room, the NSC staff, and other White House offices. WHSSS funds support the running of the information systems used by the NSC and others.

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 Executive Voice over Secure IP (VoSIP) phone network (includes the National Intelligence Watch Officers Network (NOIWON)) to the President, Vice President, National Security Advisor, and others as directed by the NSC, both in fixed and mobile modes. Funding covers the cost of maintenance, life-cycle equipment replacement, and engineering support.

d. Minimum Emergency Essential Communications Network (MEECN)

MEECN supports a highly survivable communications “system-of-systems” which is capable of transmitting Nuclear Command and Control (NC2) messages and establishing crisis conferences with the President, Vice President, Secretary of Defense, and the Chairman of the Joint Chiefs of Staff to the Commanders of the Combatant Commands and to deployed US nuclear forces. These sub-activities support the Commander in Chief (CINC) communications with Service-provided systems ranging from modern enterprise information technology to highly specialized, secure and survivable command and control components. Grouping these sub-activities together provides a management structure that ensures seamless

I. Description of Operations Financed: (continued)

engineering, plans and procedures, and operational assessment support of these capabilities. The program is increased in FY 2009 and out to support additional mission support requirements.

e. Communications Management Control Activity (CMCA)

CMCA provides 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 civilian salary as well as minor equipment purchases and miscellaneous contract support.

II. Force Structure Summary: N/A

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

III. Financial Summary ($ in thousands)

		FY 2008					
			Congressional Action				
A. BA Subactivities	FY 2007 Actuals	Budget Request	Amount	Percent	Appropriated	Current Estimate	FY 2009 Estimate
1. Transition to Net Centric Environment	94,483	93,339	-5,044	-5.40%	88,295	88,295	170,850
2. Eliminate Bandwidth Constraints	235,324	144,195	4,015	2.78%	148,210	167,129	156,915
3. GIG Network Operations and Defense	331,819	336,007	-12,421	-3.70%	323,586	323,586	443,353
4. Exploit the GIG for Improved Decision Making	197,714	159,538	-166	-0.10%	159,372	159,372	233,349
5. Deliver Capabilities Effectively/Efficiently	109,725	66,552	-3,143	-4.72%	63,409	63,409	68,466
6. Special Missions	127,079	145,963	-3,168	-2.17%	142,795	142,795	154,693
Total BA 4	**1,096,144**	**945,594**	**-19,927**	**-2.11%**	**925,667**	**944,586**	**1,227,626**

* The FY 2007 Actual column includes $28,000 thousand of FY 2007 Global War on Terror Emergency Supplemental funds (PL 110-28), $56,939 thousand of Iraq Freedom Fund transfers, $38,600. thousand of FY 2007 Title IX funds (PL 109-289), and $2,900 of Spectrum Relocation funds.

** The FY 2008 Estimate column includes $18.919 million of X-year funding for Spectrum Relocation, excludes $44,510 thousand of GWOT funds received from the Consolidated Appropriations Act of 2008 (HR 2764/PL 110 – 15) out of the total GWOT request of $175,000 thousand.

III. Financial Summary ($ in thousands)

B. Reconciliation Summary	Change FY 2008/FY 2008	Change FY 2008/FY 2009
Baseline Funding	**945,594**	**1,118,008**
Congressional Adjustments (Distributed)	0	0
Congressional Adjustments (Undistributed)	-14,791	-83
Adjustments to Meet Congressional Intent	-419	0
Congressional Adjustments (General Provisions)	-4,717	0
Subtotal Appropriated Amount	**925,667**	**1,117,925**
Fact-of-Life Changes (CY to CY Only)	0	7,975
Subtotal Baseline Funding	**925,667**	**1,125,900**
Anticipated Supplemental	44,510	
No-year carryover	18,919	
Price Changes		
Functional Transfers		-387
Program Changes		102,113
Current Estimate	**989,096**	**1,227,626**
Less: Wartime Supplemental and Spectrum Relocation Funding	-63,429	0
Normalized Current Estimate	**925,667**	**1,227,626**

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
FY 2008 President's Budget Request (Amended, if applicable)		**945,594**
1. Congressional Adjustments		
a. Distributed Adjustments		-19,927
b. Undistributed Adjustments	-14,791	
c. Adjustments to meet Congressional Intent		
d. General Provisions		
1) Sec 8097 – Contractor Efficiencies	-1,527	
2) Sec 8104 – Economic Assumptions	-3,190	
e. Congressional Earmarks – Indian Lands Environmental Impact	-419	
FY 2008 Appropriated Amount		**925,667**
2. War-Related and Disaster Supplemental Appropriations		44,510
3. Fact of Life Changes - Spectrum Relocation Funding		18,919
FY 2008 Baseline Funding		**989,096**
4. Reprogrammings (requiring 1415 Actions)		
Revised FY 2008 Estimate		**989,096**
5. Less: Item 2, War-Related and Disaster Supplemental Appropriations and Item 3 Spectrum Relocation Funding		-63,429
FY 2008 Normalized Current Estimate		**925,667**
6. Price Change		21,897
7. Functional Transfers		17,903
a. Transfers In		
1) Funding Transferred to DISA from Services and Business Transformation (BTA) to support computer hosting costs	13,790	
2)Transfers In - Realignment of resources between DISA, DWCF and O&M,D-W	4,500	
b. Transfers Out - Transfer of responsibility for supporting the Army Net-Centric Data Management Program (ANCDMP) from DISA to the Army CIO/G-6.	-387	
8. Program Increases		
a. Annualization of New FY 2008 Program		
b. One-Time FY 2009 Increases		43,129
1) DISN: Adjustment to Customer Funding for DISN Services	2,000	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
2) CENTRIXS: CENTRIXS will support efforts to consolidate networks for coalition partners that will allow the secure sharing of mission specific information	14,610	
3) NCES: Increased funding to add defense users to Knowledge Online	7,600	
4) Spectrum Relocation Funding	18,919	
c. Program Growth in FY 2009		236,627
1) NCES: Increase sustainment efforts of the different NCES core enterprise services as they migrate from a developmental state to an operational stage (FY 2008 Base: $26,595 thousand)	55,085	
2) GIG Engr Services: Funding increased due to applying an Enterprise Wide Systems Engineering (EWSE) approach to the GIG capabilities that will enable improved Department-wide acquisition decisions based on solid technical recommendations (FY 2008 Base: $54,798 thousand)	16,925	
3) Other Program Support: Increase in support requirements as ACTDs transition and ACTD New Starts come on-line; increase in personnel requirements for new initiatives; support for CWID operational support requirements; and increased funding to support organizational activities required to run the agency and support the major programs and functions in their efforts to deliver capability to the warfighter and other customers (FY 2008 Base: $161,321 thousand)	5,848	
4) DISN: Increase for additional circuit transitions based on projected workload (FY 2008 Base: $102,578 thousand)	1,160	
5) Network Ops: Increase for integration and synchronization support of the Agency's TNC/CNOSC transformation initiatives to ensure timely capabilities improvements, improved efficiencies and business practices, end-to-end interoperability and reliability. (FY 2008 Base: $6,855 thousand)	10,200	
6) ISSP/PKI: Increase for supplies and materials, equipment operation and maintenance contracts, facility operation and maintenance contracts, equipment purchases, consultant contracts, and engineering and technical services needed to support and implement upgrades (FY 2008 Base: $247,683 thousand)	58,637	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
7) Comprehensive National Cybersecurity Initiative (FY 2008 Base: $0 thousand)	38,000	
8) GCCS: Increase in maintenance activities associated with the fielding of GCCS-J releases, and the continued sustainment of current version of GCCS-J until newest version is fully fielded; funding also supports internal realignment of funding to begin the migration of the JSSC to the DISA Defense Enterprise Computing Centers (DECC) in order to support net-centric operations; and to continue transition into the sustainment phase of the lifecycle (FY 2008 Base: $76,183 thousand)	11,298	
9) GCSS: Increase funds incremental implementation of a service-oriented architecture (SOA) in a net-centric environment utilizing the Net-Centric Enterprise Services (NCES) core concepts as well as other key applications (FY 2008 Base: $15,694 thousand)	1,774	
10) WHCA: Increased funding for facilities at Mechanicsburg and expected completion of modernization initiatives which will move sustainment phase and projected lifecycle replacements. (FY 2008 Base: $119,325 thousand)	8,987	
11) DMS: Increase for hardware and software maintenance to support the additional DMS Maintenance Releases (FY 2008 Base: $12,924 thousand)	2,952	
12) NECC: Increased funding to provide for a single, integrated, coherent system for operational level C2 (FY 2008 Base: $9,730 thousand)	25,761	
9. Program Decreases		-17,597
a. Annualization of FY 2008 Program Decreases		
b. One-Time FY 2008 Decreases		
c. Program Decreases in FY 2009		
1) DSO: Decrease in FY 2007 Spectrum Relocation funding received in FY 2007 (FY 2008 Base: 45,832)	-15,664	
2) DISN Technology Refresh	-900	
3) One less paid day (FY 2008 Base: 270,549)	-1,033	
FY 2009 Budget Request	1,227,626	1,227,626

IV. Performance Criteria and Evaluation Summary

DISA's principal approach to performance-budget integration and performance measurement is budgeting to our strategy and using a balanced scorecard (BSC) to manage, monitor and execute this strategy. The BSC provides a "pyramid" of outcomes structure, with DISA's Surety-Reach-Speed strategy (2nd edition, March 2007, and available on the Internet at www.disa.mil/strategy/strategy_book.pdf) and top-level goals on top. Top corporate level, or Level 1 strategy and measures, are supported by lower level strategic initiatives and measures developed by subordinate organizations. The higher-level strategy is supported with outcome-oriented as well as output measures, with targets. The customer perspective portions of the strategy and their measures are supported by financial, internal process, and learning and growth related portions of strategies and by measures. Targets are at a level that promotes continuous improvement.

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

The DISA uses other external measurement methodologies to track performance that are integrated into the DISA's budget. For example, readiness metrics and supporting data to measure readiness to execute mission essential tasks are captured under the DoD Readiness Reporting System (DRRS) required by the DoD Directive 7730.65. Strategies are developed for rectifying readiness deficiencies, and these strategies are addressed in

IV. Performance Criteria and Evaluation Summary

program/budget planning as DoD Directive 7730.65 requires. Another external measurement used is the performance and budget information for Capital Asset Plan and the Business Case Summary Exhibit 300's required by the Office of Management and Budget Circular A-11.

Primary performance targets and results for DISA are specified in the Exhibit 300's, which include actual to projected performance results for FY 2007 and planned for FY 2008 and FY 2009, and the Exhibit 300's address the Program Assessment Rating Tool (PART) process. The DISA's Teleport and Defense Information System Network (DISN) are under PART as part of the Defense Communications Infrastructure. As example of performance targets and results, for the Teleport, Teleport is being deployed incrementally in a multi-generational program. The various generations have targets for completion, and Generation Two (FY 2006 – FY 2009) adds additional military Ka band capability and implements IP Net-Centric communications at the Teleport sites. Generation 2 is proceeding as planned.

DISA's current Surety-Reach-Speed strategy focuses on aggressive leadership in five areas:

1) Speed - to deliver IT capabilities and services faster;
2) Power to edge - to push enterprise services to the edge;
3) Operational excellence - to accelerate operational effectiveness and efficiency;
4) Sharing and defense of information - to enable sharing of information while staunchly protecting it; and,
5) Best values – to assure customers know and understand the value of DISA capabilities and services.

A summary of DISA's latest BSC top-level goals/strategies for the customer perspective and the financial perspective, their linkage to the 2006 Quadrennial Defense Review (QDR)

IV. Performance Criteria and Evaluation Summary

as well as the March 2005 National Defense Strategy, the DoD risk management framework (2001 QDR), *DoD Performance and Accountability Report (PAR*) for FY 2006, and the *President's Management Agenda (PMA),* are provided below. Since DoD will include the FY 2007 PAR with the FY 2009 Congressional Budget Justification that will be submitted in February 2008, the DoD PAR FY 2006 is still used for the linkages. The QDR 2006 linkages are primarily mapped to the "Reorienting Capabilities and Forces" section of the 2006 QDR.

The text below demonstrates how DISA's performance budget is aligned to DoD's performance budget. In addition, where applicable, a brief evaluation and assessment of select key results for the DISA's last BSC used by the DISA to support ongoing decision-making is provided. 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.

DISA's top-level goals in the customer perspective are:

DISA Strategy/Goal: Deliver IT capabilities and services faster

- *Corporate Strategy*: This portion strategy includes DISA becoming the joint acquisition agent of choice for enterprise IT capabilities and services; increasing the speed and flexibility of the requirements and acquisition processes; tailoring oversight and governance to be commensurate with risk; adopting innovative ideas and processes to deliver capabilities and services that our forces are able to use with agility; and using the precepts of adopt-before-we-buy and buy-before we-create. The strategy will be measured with measures such as the percent of IT capabilities and services delivered faster and the amount of time to provision basic circuits.

IV. Performance Criteria and Evaluation Summary

This relates to the measure in DISA's previous BSC for the percentage of acquisitions capabilities that are delivered within established Acquisition Program Baselines (APB)/APB-like thresholds, where the targets are the baselines or APB-like thresholds.

- Corporate Strategy Linkages include:
  - National Defense Strategy: Continuous transformation - continually adapt how we approach and confront challenges, conduct business, and work with others.
  - QDR: Toward a New Defense Enterprise.
  - Risk Management Framework: Operational, Future Challenges, and Institutional Risk.
  - DoD PAR FY 2006:
    - Strategic Goal 3: Balance Institutional Risk - improving acquisition processes.
      - Performance Goal 3.3: Realign Support to the Warfighter
        - Metric: Reduce Major Defense Acquisition Program Acquisition Cycle Time
      - Performance Goal 3.4: Streamline the Decision Process, Improve Financial Management, and Drive Acquisition Excellence
  - 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 Strategy/Goal: Extend services to the Edge

Corporate Strategy: This portion strategy includes the need for enterprise wide systems engineering, a single concept of operations for network operations, Net-Centric Enterprise Services (NCES), Net-Enabled Command Capability (NECC), NetOps, scalable net-

IV. Performance Criteria and Evaluation Summary

centric computing, terrestrial and satellite communications, and transforming spectrum management. This relates to the measure in the DISA's previous BSC for the percent of capabilities incorporating net-centric attributes, where target goals were 80 to 100 percent, depending upon the portfolio, and the investments on the list of eligible programs were all on track. It relates to previous BSC measures for the number of circuits transitioned to new core and number of circuits discontinued, achieving NetOps criteria, and implementing the Net Common Operational Picture.

- Corporate Strategy Linkages include:
  - National Defense Strategy: Operating from the global commons; Conducting network-centric operations.
  - QDR: Achieving Net-Centricity, Joint Command and Control, Tailored Deterrence/ New Triad and Defeating Terrorist Networks, and Shaping the Choices of Countries at Strategic Crossroads.
  - Risk Management Framework: Operational and Future Challenges.
  - DoD PAR FY 2006 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.
      - 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.

IV. Performance Criteria and Evaluation Summary

DISA Strategy/Goal: Accelerate operational effectiveness and efficiency

- *Corporate Strategy*: This portion strategy includes excellence in customer relationships and the agility required to adjust to dynamic requirements, partnering with customers, simplifying the business model for cost recovery of DISA services, increasing communication with user community through improved web and web-services access and services status, and making DISA's enterprise computing centers dramatically different. The strategy will be measured with measures such as the cost of network management for the DISN versus the total cost of the DISN, number of employees and contractors engaged in network management, network performance DISN core availability, and percentage of DISA-provided services and capabilities visible to a NetOps center.
- Corporate Strategy Linkages include:
  - National Defense Strategy: Continuous transformation - continually adapt how we approach and confront challenges, conduct business, and work with others.
  - QDR: Toward A New Defense Enterprise.
  - Risk Management Framework: Operational, Future Challenges, and Institutional Risk.
  - DoD PAR FY 2006
    - Strategic Goal 3: Balance Institutional Risk - improving acquisition processes.
      - Performance Goal 3.3: Realign Support to the Warfighter
        - Metric: Reduce Major Defense Acquisition Program Acquisition Cycle Time
    - DoD PAR FY 2006 Strategic Goal 4: Balancing Future Challenges Risks - execute future missions successfully against an array of prospective challengers

IV. Performance Criteria and Evaluation Summary

- Performance Goal 4.1 Define and develop transformational capabilities.
  - 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 President's Management Agenda (PMA): Expanded Electronic Government.

DISA Strategy/Goal: Enable sharing of information while staunchly protecting it

- *Corporate Strategy*: This portion strategy includes aggressively developing and implementing measures to manage and defend the global information grid (GIG) to ensure warfighting forces, including partners and allies, can deploy and connect globally, and share timely, trusted, and accurate information needed for their missions. The strategy will be measured with measures such as the percentage of facing web services hosted in DoD demilitarized zones (DMZs).
- Corporate Strategy Linkages include:
  - *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 2006 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.
      - Metric 4.1.2 Make Information Available on a Network that People Depend On and Trust/ Number of systems that support the Internet

IV. Performance Criteria and Evaluation Summary

Protocol Version 6 (IPv6) and Number of systems that meet information assurance standards.

- o President's Management Agenda (PMA): Expanded Electronic Government.
- o DISA's Surety-Reach-Speed Strategy: DISA's Surety-Reach-Speed Strategy leadership area of sharing and defense of information to enable sharing of information while staunchly protecting it.

DISA's top-level goal in the financial perspective is:

DISA Strategy/Goal: Best value – customers know and understand the value of DISA capabilities and services

- *Corporate Strategy*: This portion strategy includes excelling in stewardship of taxpayer dollars through integrity, full and open financial disclosure, fiscal discipline, and professional competency. The strategy will be measured with measures such as disbursement rates, obligation rates, milestones toward achieving a clean audit opinion, and timeliness of budget inputs.
- Corporate Strategy Linkages include:
  - o National Defense Strategy: Continuous transformation - continually adapt how we approach and confront challenges, conduct business, and work with others.
  - o QDR: Toward A New Defense Enterprise.
  - o Risk Management Framework: Operational, Future Challenges, and Institutional Risk.
  - o DoD PAR FY 2006
    - ▪ Strategic Goal 3: Balance Institutional Risk - improving acquisition processes.

IV. Performance Criteria and Evaluation Summary

- Performance Goal 3.4: Streamline the Decision Process, Improve Financial Management, and Drive Acquisition Excellence

o President's Management Agenda (PMA): Expanded Electronic Government, Budget Performance Integration

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

V. Personnel Summary

	FY 2007	FY 2008	FY 2009	Change FY 2007 FY 2008	Change FY 2008 FY 2009
Active Military End Strength (E/S) (Total)	1,502	1,456	1,456	-46	0
Officer	359	340	340	-19	0
Enlisted	1,143	1,116	1,116	-27	0
Reserve Drill Strength (E/S) (Total)	103	93	93	-10	0
Officer	61	51	51	-10	0
Enlisted	42	42	42	0	0
Reservists on Full Time Active Duty (E/S)	2	1	1	-1	0
Officer	1	1	1	0	
Enlisted	1	0	0	-1	0
Civilian End Strength (Total)	2,544	2,412	2,413	-132	1
U.S. Direct Hire	2,458	2,307	2,308	-151	1
Foreign National Indirect Hire	5	5	5	0	0
Memo: Reimbursable Civilians Included	81	100	100	19	0
Civilian FTEs (Total)					
U.S. Direct Hire	2,385	2,291	2,292	-94	1
Foreign National Indirect Hire	5	5	5	0	0
Memo: Reimbursable Civilians Included	75	85	85	10	0
Foreign National Indirect Hire	5	5	5	0	0
Memo: Reimbursable Civilians Included	81	100	100	19	0
Average Annual Civilian Salary($ in thousands)	111.4	119.3	122.9	7.9	3.6

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

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

OP 32 Line		FY 2007 Actuals	Change from FY 2007 to FY 2008 Price Growth	Change from FY 2007 to FY 2008 Program Growth	FY 2008 Estimate	Change from FY 2008 to FY 2009 Price Growth	Change from FY 2008 to FY 2009 Program Growth	FY 2009 Estimate
	CIVILIAN PERSONNEL COMPENSATION							
101	Executive, Gen'l and Special Schedules	264,879	6,788	-1,118	270,549	8,910	945	280,404
103	Wage Board	18	0	-18	0	0	0	0
106	Benefits to Former Employees	0	0	0	0	0	0	0
107	Voluntary Separation Incentive	0	0	1,500	1,500	0	-1,500	0
111	Disability Compensation	828	0	325	1,153	0	58	1,211
121	Permanent Change of Station	0	0	0	0	0	0	0
199	Total CivPers Compensation	265,725	6,788	689	273,202	8,910	-497	281,615
	TRAVEL							
308	Travel of Persons	25,539	485	11,904	37,928	759	5,315	44,002
399	Total Travel	25,539	485	11,904	37,928	759	5,315	44,002
	OTHER FUND PURCHASES (EXCLUDE TRANSPORTATION)							
672	Pentagon Reservation Maintenance	15,471	-743	-586	14,142	438	127	14,707
673	Defense Finance and Accounting Services	7,184	-345	-275	6,564	-341	2,365	8,588
677	Communications Services Tier 1	15,897	606	-1,134	15,369	-792	-262	14,315
699	Total Purchases	38,552	-482	-6,598	31,472	-463	6,601	37,610
	TRANSPORTATION		0			0		
771	Commercial Transportation	1,975	43	899	2,917	61	179	3,157
799	Total Transportation	1,975	43	899	2,917	61	179	3,157
	OTHER PURCHASES							
912	Rental Payments to GSA (SLUC)	20,268	507	-3,595	17,180	430	1,715	19,325

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

OP 32 Line		FY 2007 Actuals	Change from FY 2007 to FY 2008 Price Growth	Change from FY 2007 to FY 2008 Program Growth	FY 2008 Estimate	Change from FY 2008 to FY 2009 Price Growth	Change from FY 2008 to FY 2009 Program Growth	FY 2009 Estimate
913	Purchased Utilities (non-Fund)	3,412	65	-137	3,340	67	146	3,553
914	Purchased Comm (Non-Fund)	40,541	770	-11,043	30,268	605	8,991	39,864
915	Rents (Non-GSA)	202	4	-91	115	2	-2	115
917	Postal Services (U.S.P.S.)	160	0	68	228	0	7	235
920	Supplies & Materials (Non-Fund)	11,668	222	-2,040	9,850	197	3,183	13,230
921	Printing & Reproduction	364	7	-82	289	6	0	295
922	Equipment Maint by Contract	511,372	9,716	-114,630	406,458	9,019	177,586	593,063
923	Facility Sustain, Restor'n, and Modernization by Contract	20,091	382	-9,697	10,776	216	386	11,378
925	Equipment Purchases (Non-Fund)	48,165	915	-14,637	34,443	689	16,177	51,309
931	Contract Consultants	418	8	888	1,314	26	-25	1,315
932	Mgmt & Prof'l Support Services	2,392	45	-2,192	245	5	3	253
933	Studies, Analysis, & Evals	194	4	99	297	6	2	305
934	Engineering & Tech Services	1,666	32	4,246	5,944	119	109	6,172
937	Local Purchase Fuel (Non-Fund)	0	0	0	0	0	0	0
987	Other Intra-gov't Purchases	29,086	553	-11,402	18,237	365	15,758	34,360
988	Grants	135	3	-99	39	1	0	40
989	Other Contracts	74,024	1,406	-20,033	55,397	1,108	29,880	86,385
998	Other Costs	195	4	-155	44	1	0	45
999	Total Other Purchases	764,353	14,643	-184,532	594,464	12,862	253,916	861,242
9999	**TOTAL**	**1,096,144**	**21,477**	**-173,035**	**944,586**	**21,897**	**261,143**	**1,227,626**

* The FY 2007 Actual column includes $28,000 thousand of FY 2007 Global War on Terror Emergency Supplemental funds (PL 110-28), $56,939 thousand of Iraq Freedom Fund transfers, $38,600. thousand of FY 2007 Title IX funds (PL 109-289), and $2,900 of Spectrum Relocation funds.

** The FY 2008 Estimate column includes $18.919 million of X-year funding for Spectrum Relocation, excludes $44,510 thousand of GWOT funds received from the Consolidated Appropriations Act of 2008 (HR 2764/PL 110 – 15) out of the total GWOT request of $175,000 thousand.

This page intentionally left blank.