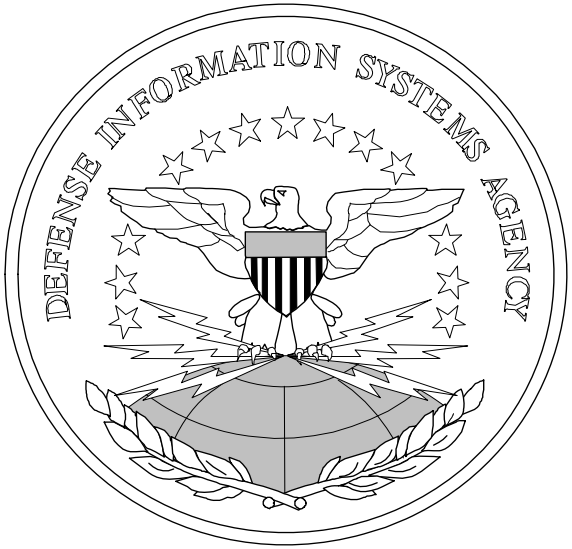
Fiscal Year 2010 Budget Estimates
Defense Information Systems Agency (DISA)



May 2009

(This page intentionally left blank.)

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2010 Budget Estimates

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

	FY 2008 Actuals	Price Change	Program Change	FY 2009 Estimate	Price Change	Program Change	FY 2010 Estimate
DISA	1,104,173	20,948	71,436	1,196,557	17,386	108,220	1,322,163

*The FY 2008 Actual column includes $44,510 thousand of Consolidated Appropriations Act, 2008, Division L, Supplemental Appropriations, Defense (PL 110-161), $105,794 thousand of Supplemental Appropriations Act, 2008, Title IX, Defense Matters, Chapter 1, Defense Supplemental Appropriations for Fiscal Year 2008 (PL 110-252), and includes $3,611 thousand of No-Year Spectrum Relocation funds.
**The FY 2009 column excludes $31,100 thousand of Bridge Funding Appropriations for FY 2009 (PL 110-329), $118,705 thousand of FY 2009 Overseas Contingency Operations funding, and also excludes $15,309 thousand of No-Year Spectrum Relocation funds.
***The FY 2010 column excludes the request for $245,117 thousand of Overseas Contingency Operations funding.

I. Description of Operations Financed: The Defense Information Systems Agency (DISA) is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global information sharing solutions. The DISA also operates the Global Information Grid (GIG) to serve the needs of its customers, including, the President, Vice President, the Secretary of Defense, the Joint Chiefs of Staff, the Combatant Commanders (COCOMS), and other Department of Defense (DoD) components during peace and war times. The DISA operates under the direction, authority, and control of the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)). The DISA Director's dual role as the Commander, Joint Task Force-Global Network Operations (JTF-GNO) assigns additional responsibility for directing the operation and defense of the GIG. In short, DISA provides global net-centric solutions for the Nation's warfighters and the support services in the defense of the nation.

The DISA's program implements the Secretary of Defense's (SECDEF) Guidance for the Development of the Force (GDF) and reflects the DoD, Chief Information Officer's Information Sharing Strategy. The DoD CIO vision for information sharing is, "Deliver the power of information to ensure mission success through an agile enterprise with

I. Description of Operations Financed: (continued)

freedom of maneuverability across the information environment." This vision synchronizes initiatives to share information among DoD components, across levels of U.S. government, international coalition partners, and the private sector.

This concept delivers on the three overarching goals of the DISA strategy:

- Surety – information is available when and where needed
- Reach – warfighting forces can deploy and connect to the network no matter the location, pull information needed for the missions, and be given timely, accurate information on any threats
- Speed – deliver IT capabilities and services faster

The DISA primary mission is to aggressively innovate and facilitate a collaborative GIG environment to provide virtual information on demand in a global network-centric operation in five areas:

- Sharing and defense of information – enables sharing of information while steadfastly protecting it
- Speed – deliver IT capabilities and services faster
- Power to edge – extend services to the edge (The vision of "power to the edge" is the availability of a "ubiquitous, secure, robust, trusted, protected, and routinely used wide-bandwidth that is populated with the information and information services that the forces need)
- Operational excellence – accelerate operational effectiveness and efficiency
- Best value – customers know and understand the value of DISA capabilities and services

I. Description of Operations Financed: (continued)

The DISA aligns its mission, essential tasks, goals and strategies, and program resource structure across six mission areas. The first five mission areas reflect the customer support strategies of the DISA Balanced Scorecard, the sixth mission area represents DISA's critical special mission to support the Commander in Chief. These mission areas reflect the DoD goals and represent DISA's focus on key activities.

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.
3. Operate, manage, and defend the GIG to enhance critical warfighting and business capabilities in a secure, net-centric environment.
4. Transition to DoD enterprise-wide capabilities, 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.
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 DISA continues to use the Total Cost Allocation Model to assign costs of shared services to products and services. The Cost Allocation Model identifies the total cost of a program and avoids unintended subsidy to the Defense Working Capital Fund, gains visibility and insight into cost and consumption of shared services, and addresses efficiencies.

I. Description of Operations Financed: (continued)

The DISA is aggressively implementing measures to manage and defend the GIG to ensure warfighting forces (partners and allies) can deploy and connect globally, and share timely, trusted, and accurate information needed for the mission. The DISA will propose policy and implement instructions for security certification and accreditation supporting the fast-paced, nearly ad hoc, on-demand nature of net-centric operations and warfare. Achieving these goals requires DISA to synchronize efforts with partners to extend capabilities and services to the edge that aids DoD in fostering collaborative networks that enable the effects-based fight. Achieving these goals requires an enterprise-wide systems strategy, architecture, and a single concept of operations for network operations, configuration control, and situational awareness. The DISA continues the adopt-before-buy and buy-before-create approach as a way of getting the 80 percent solution in the hands of the warfighter quickly.

Significant Program Changes: The total net change between FY 2009 and FY 2010 is $125,606 thousand (+$17,386 thousand in price change and +$108,220 thousand in program change). The significant increases in funding were for classified programs (+$65,331 thousand); national cyber security initiative mission (+$30,715 thousand); the single centrally-managed network for U.S. and Coalition forces (+$8,140 thousand); innovation and decision making efforts (+$17,300 thousand); operational requirements for NCES (+$18,749 thousand); next Generation Teleport (+$2,100 thousand); AFRICOM initiatives (+$3,500 thousand); decrease in fielding requirements for GCCS-J (-$22,881 thousand); Congressional and other reductions to the Net-Enabled Command Capability (NECC) program (-$1,386 thousand); and 50 Full Time Equivalent (FTE) increase starting in FY 2010 (realignment from non-pay to pay). The remaining decreases (-$11,821 thousand) are net changes in operational support requirements, rent adjustments, vendor requirements, and an Agency-wide rebaseline of civilian pay and benefits to adequately reflect payroll costs for each program as DISA transitions to a

I. Description of Operations Financed: (continued)

Manage-to-Pay concept that was initiated in FY 2009. In FY 2010, DISA intends to replace approximately 4 contractors with approximately 8 government employees at a total cost savings of $1,527.

Descriptions of Operations Financed by Mission Area:

1. Transition to Net-Centric Environment:

Mission Area Component ($ in Thousands)	FY 2008	FY 2009	FY 2010
a. Net-Centric Enterprise Services	34,021	89,247	117,025
b. GIG Engineering Services	46,600	73,249	69,524
c. Advanced Concept Technology Demonstration	11,001	5,889	11,368
d. Coalition Warrior Interoperability Demonstration	2,410	2,194	2,286
e. Other Programs	721	0	0
Transition to Net Centric Environment Total	**94,753**	**170,579**	**200,203**

a. Net-Centric Enterprise Services (NCES): (FY 2010: $117,025 thousand) The Program Executive Office (PEO) for GIG Enterprise Services (GES) requests FY 2010 funding to provide enterprise services to the Combatant Commands (COCOMS), Services, Joint Staff, the Office of the Secretary of Defense, Defense wide agencies, and the Warfighter, Business, and Intelligence Mission Areas. In FY 2010, NCES will expand from support to one Program of Record (POR), NCES, to a portfolio of programs including NCES, persistence presence, the Vice-Chairman of the Joint Chiefs of Staff initiatives, and engineering innovative initiatives.

I. Description of Operations Financed: (continued)

The FY 2010 funding will move NCES capabilities in the product lines through a Full Deployment Decision Review with follow-on fielding decisions as required. NCES will be building the services out to Initial Operational Capability (IOC) levels and performing threshold requirements validation in the NCES Capability Production Document (CPD).

The NCES Program Office Estimate for FY 2010 is $109,025, major efforts include:

- $27,750 thousand: The GIG Content Delivery Service (GCDS) migration from 9X5 to 24x7 support with the required IOC level of 26 edge nodes on the SIPRNET and 26 on the NIPRNET and 25 Uniform Resource Locators (URLs) available on each network to support forward caching of critical information;
- $29,285 thousand: The projected growth of Collaboration Web Conferences peak concurrent usage on the SIPRNET by 35 percent and 55 percent on the NIPRNET and Chat/Instant Messaging capabilities on the SIPRNET by 35 percent and 61 percent on the NIPRNET as documented in the NCES Life Cycle Cost Estimate (LCCE);
- $11,105 thousand: Build-out of the User Access (Portal) infrastructure on Defense Knowledge Online to support the remaining 1 million user seats of the total 2.5 million population that NCES will support at Full Operational Capability (FOC);
- $25,101 thousand: Expansion of Service Oriented Architecture Foundation (SOAF) to support the PORs that are using the services; and expansion of Discovery services on the NIPRNET and enhancement of services on the SIPRNET and NIPRNET. During this period, the NCES Program Management Office (PMO) will realign 15 percent of the civilian staff positions as shown in the Program Office Estimate (POE) due to the migration of the services into the deployment and production environment.

In FY 2010, NCES will receive 10 additional FTEs to manage the Innovative Initiatives Office. The increase of $8,000 will provide resources to perform engineering innovation of rapid solutions that enables warfighting operational transformation with engineering

I. Description of Operations Financed: (continued)

innovation. This includes advanced data, enterprise information and knowledge services, development, and operational structures in the following areas: acceleration of commercial internet concepts and technology; development of advanced senior leader decision support capabilities, improved global situational awareness, expanded enterprise services to support tactical collaboration and data processing services; development of integrated NetOps services, and to develop trusted access, application and data services.

b. GIG Engineering Services (GIG ES): (FY 2010: $69,524 thousand) The Systems Engineering Center (SEC) provides architecture, systems engineering and end-to-end analytical functions for the DISA and its customers, enabling integrated capabilities to fulfill warfighter mission requirements. The SEC O&M funds, (FY 2010: $68,912) to accomplish the following tasks to the Net-Centric Environment:

- Develop, implement, and continuously improve on net-centric SE processes;
- Develop a DISA Strategic Technology Roadmap (DSTR) process outlining an approach to identify, characterize, and provide guidance on strategic technologies;
- Identify and develop the net-centric standards for GIG Transport and Enterprise Services;
- Provide technical standards direct support to the DISA PEOs to capture and promulgate net-centric technical implementation profiles for DoD-wide use;
- Assess Net-Centric Certification under Joint Capabilities Integration and Development System (JCIDS) requirements to capture the state of interoperability of systems in a joint/combined/coalition net-centric environment;
- Effect messaging standards transition to net-centric environment;
- Develop and expand virtual program assessment capabilities under the Joint C4 Program Assessment Tool (JCPAT) to capture program compliance and implementation data with the GIG Technical Documentation (GTD); and

I. Description of Operations Financed: (continued)

- Maintain a modeling and simulation environment and capabilities to support the evolving DISN and other major DISA programs and projects.

The 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. The SEC develops across-theater information awareness for COCOMS through application solutions for integrated networks, which include missions in Iraq and Afghanistan, by:

- Supporting the development and implementation of GIG Enterprise-Wide Systems Engineering (EWSE) processes and technical direction that enable interoperability and end-to-end performance;
- Developing and maintaining a standardized DISA systems engineering and integration process to improve systems integration across DISA;
- Developing, maintaining, and supporting the identification of all individual IT commercial, military (MILSTD), international (NATO) standards and associated enterprise architectures under the Defense Information Technology Standards Registry (DISR); and
- Providing the underlying modeling and simulation and analytical support for end-to-end DISA and DoD systems engineering and assessment.

Another component of GIG Engineering Services is the Chief Technology Officer (CTO) (FY 2010: $612). The CTO supports efforts to strengthen the delivery of critical GIG products, services, and capabilities to the warfighter through the establishment of DISA technology positions, strategies, and roadmaps, technology development and insertion into DISA programs of record while also influencing Service/Agency program technology

I. Description of Operations Financed: (continued)

investments. This project is provides a crucial capability that ensures engineering rigor, technical soundness, and alignment with GIG architectural constructs in the products, services, and capabilities delivered to the Services, COCOMS, OSD, and the Joint Staff. The CTO project conducts a multi-tiered approach to technical research and analysis which includes identification of near-term critical technical solutions, mid-term technology investments, and long-term, high-potential over-the-horizon technology innovation. The CTO project will support Technology Readiness Assessments (TRA); technology analysis and demonstrations involving cloud computing, service oriented architecture, and GIG 2.0; focused technology tiger teams to develop a design and execution plan for the next generation DoD intranet infrastructure; technology integration and insertion into programs of record; and technology positions, strategies, and roadmaps.

c. Advanced Concepts Technology Demonstrations (ACTDs) and Joint Capability Technology Demonstrations (JCTDs)(FY 2010: $11,368 thousand): The objective of the Innovation Technology Transformation (IT2) Program is to demonstrate and integrate new, mature Information Technology (IT) and advanced operational concepts into net-centric battle space technologies in order to access and exchange critical information, exploit opportunities to enhance Current Force capabilities, and project Future Force IT requirements. The focus is on responding to and meeting emergent warfighter requirements in an innovative, collaborative method and put the new or improved capabilities in the hands of the warfighter in a rapid manner. The DISA leverages existing Programs of Record (POR) and enterprise service environments to speed implementation time and improve return on investment.

The FY 2010 funding will support an increased capability to deliver prioritized emergent IT faster, extend enterprise services, accelerate operational effectiveness and

I. Description of Operations Financed: (continued)

efficiency, and enable information sharing and assurance. The program utilizes three key mechanisms to streamline the process of fielding emergent requirements: (1) Advanced Concept Technology Demonstrations (ACTD) /Joint Capability Technology Demonstrations (JCTD), with OSD/COCOMs/Service/Agency teaming; (2) Joint Ventures, with Combatant Commanders/Program of Record (POR) teaming; and (3) Risk Mitigation Pilots, with POR/Community of Interest (COI) teaming.

The DISA CTO's endeavors will provide senior military leadership with (1) the ability to support senior-level initiatives; (2) the capability to maintain global situational awareness of leading edge technologies; (3) the capability to rapidly field solutions to emerging problems; and (4) the benefit of securing a competitive edge through intellectual capital. The ITTP provides critical new customer focus on the long-term global war on terrorism via the confluence of technology, security cooperation, and education. The program components support preparation for future joint and coalition initiatives through development and integration of a full range of data services and advanced IT applications to support practical aspects of United States and coalition partner approved cooperative activities.

d. Coalition Warrior Interoperability Demonstration (FY 2010: $2,286 thousand): This funding is for the Coalition Warrior Interoperability Demonstration (CWID) directed by the Joint Chiefs of Staff (CJCS) to find solutions to urgent, existing gaps and weaknesses (as identified by the uniformed services, combatant commanders, DoD agencies and others) in the DoD's command and control capabilities to interoperate with coalition partners. This is achieved by planning an operational event designed as a multinational test scenario with context to accurately evaluate and assess technologies in development by private industry and the government. Funding increases are from requirements to assess and evaluate emerging technologies. The test is scheduled for June 2010.

I. Description of Operations Financed: (continued)

2. Eliminate Bandwidth Constraints:

Mission Area Component ($ in Thousands)	FY 2008	FY 2009	FY 2010
a. DoD Teleport Program	7,401	17,279	10,543
b. Standardized Tactical Entry Point (STEP)	10,956	1,511	1,408
c. Global Electromagnetic Spectrum Information System	1,347	3,389	2,521
d. Defense Spectrum Organization	26,996	26,774	29,338
e. Defense Information Systems Network Enterprise Activities	195,418	91,576	90,053
f. Defense Information Systems Network Subscription	14,716	16,302	13,902
Eliminate Bandwidth Constraints Total	**256,834**	**156,831**	**147,765**

a. DoD Teleport Program (FY 2010: $10,543 thousand): Teleport is a collaborative investment in DoD to provide deployed warfighters with seamless worldwide multi-band Satellite Communication (SATCOM) reach-back capabilities to the Defense Information System Network (DISN). Each Teleport investment increases the warfighters' ability to communicate with a globally interconnected set of information capabilities, which is vital for the DoD to maintain a presence among its adversaries. Teleport is being deployed incrementally in a multi-generational program and upgrades selected sites from the Standardized Tactical Entry Point (STEP) program. The first generations add communications support and commercial SATCOM frequency bands that represent a ten-fold increase to the throughput and functional capabilities of these STEP sites. Previous funding provided for Generation 1 fields capabilities in four Initial Operation Capability (IOC) increments and the Generation 2 provides additional military Ka band capability.

I. Description of Operations Financed: (continued)

The Generation Three program integrates the Advanced Extremely High Frequency (AEHF) and the Mobile User Objective System (MUOS) satellite systems' capabilities into the DoD gateway architecture. This will increase satellite connectivity through technology refresh of older communication equipment suites, and adds a Teleport site in Pacific Command (PACOM) to expand the DoD gateway's capacity, throughput, and functional capabilities in support of worldwide tactical and deployed warfighters.

This funding supports an additional 12 FTEs to begin implementation of the four essential areas of Generation Three and provide program management support such as office supplies, equipment, travel, help desk, and In-Service Engineering Agent (ISEA) efforts with Program Manager Defense Communications and Army Transmission Systems (PM DCATS) and Space and Naval Warfare Systems command (SPAWAR).

b. Standarized Tactical Entry Point (STEP) (FY 2010: $1,408 thousand)**:** STEP is a DoD Satellite Communications (SATCOM) Gateway that links the deployed Warfighter to the DISN sustaining base. The STEP provides extremely high-throughput, X-Band, multi-media telecommunications services for deployed forces during operations and exercises. The STEP provides a centralized integration capability, contingency capacity, and interfaces to access the DISN in a seamless, interoperable, and economical manner. It incorporates the Joint Communications Support Element (JCSE) IP Convergence Suite into a DISN-TE (Tactical Edge) IP-based architecture that provides legacy and converged DISN services to authorized, deployed customers of DoD Gateways, and reduces the number of stovepipe solutions into a single architecture. The program is in sustainment, with funding paying for lease costs for circuits, system equipment maintenance, engineering support, data base management, training, testing, and operation of a web based portal.

I. Description of Operations Financed: (continued)

c. Global Electromagnetic Spectrum Information System (FY 2010: $2,521 thousand): The Global Electromagnetic Spectrum Information System (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 de-conflicting competing mission requirements for spectrum use. This capability will enable the transformation from the current preplanned and static frequency assignment strategy into autonomous and adaptive spectrum operations. GEMSIS will provide a long-term solution for spectrum management of a family of spectrum capabilities that will support all levels of warfare (strategic, operational, and tactical). 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.

In FY 2010, the GEMSIS PMO will continue to field GEMSIS Increment 1 capabilities to all major geographical Combatant Commands. The PMO will also sustain fielded items (CJSMPT and HNSWDO) to include logistics management, training, centralized help desk, data and database management, continuity of operations, and system certification and accreditation and execute PMO plans and processes to support previously described activities.

d. Defense Spectrum Office (FY 2010: $29,338 thousand): The Defense Spectrum Organization (DSO) is responsible for developing comprehensive and integrated spectrum planning and long-term strategies to address current and future needs for DoD electromagnetic (EM) spectrum access. The DSO supports DoD on national and international spectrum issues, spectrum coordination, and in the pursuit of emerging spectrum-efficient technologies in DoD acquisitions. The DSO serves as the DoD center of excellence for EM spectrum management, planning, policy implementation, and operational matters, and provides direct support to the ASD (NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, COCOMs,

I. Description of Operations Financed: (continued)

Secretaries of Military Departments (MILDEPs), and Directors of Defense Agencies. The DSO was established by merging and realigning the spectrum assets and resources of DISA's Defense Spectrum Office, hereafter referred to as the Strategic Planning Office (SPO), and the Joint Spectrum Center (JSC). On October1, 2008, the Global Electromagnetic Spectrum Information System (GEMSIS) Program Office was transferred to the DSO, thus consolidating all DISA EM spectrum activities in one organization.

The Strategic Planning Office's (SPO) (FY 2010: 10,397) mission is to provide integrated strategies, policies, processes, and practices to achieve global spectrum access for national security obligations. The SPO provides comprehensive and integrated spectrum planning strategies for DoD by improving EM spectrum management and electromagnetic environmental effects (E3) business processes, updating spectrum supportability roles and responsibilities throughout the spectrum management community, and enhancing acquisition and requirements processes to assure spectrum access. The SPO promotes EM spectrum and Electromagnetic Environmental Effects (E3) awareness and education through outreach programs; advocates and defends DoD's EM spectrum needs in national and international EM spectrum forums by developing and executing realistic allocation/reallocation strategies; provides proactive DoD preparation for the World Radiocommunication Conference (WRC); and integrates spectrum-related technology issues in national and international policy development and execution. The SPO is leading efforts to transform spectrum management to support current and future net-centric operations and warfare.

This funding will continue the transformation efforts supported by the Defense Spectrum Management Architecture (DSMA); the Spectrum Requirements Generation Process; strategic planning; the Presidential Spectrum Policy Initiative (PSPI); legislative support to ASD/NII; international deliberations with the WRC, the North Atlantic Treaty Organization

I. Description of Operations Financed: (continued)

(NATO) and the Combined Communications-Electronics Board (CCEB); and satellite coordination.

The Joint Spectrum Center's (JSC) (FY 2010: $18,941) mission is to enable DoD's effective use of the EM spectrum in support of national security and military objectives. The funding is responsible for developing and maintaining DoD standard information systems that support DoD spectrum related activities and processes. Specifically, JSC designs, develops, and maintains DoD automated spectrum management systems, evaluation tools, and databases employed by DoD. The JSC databases are the prime sources of information for DoD use of the EM spectrum. The JSC provides technical measurement and analysis 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. Additional focus is centered on improving future warfighter EM spectrum utilization through technological innovation accomplished by researching, studying, and steering the direction of research and development (R&D) emerging technology efforts from a spectrum perspective. The JSC is the DoD focal point for E3, and EM interference resolution assistance to operational units including deployable support to COCOM Joint Task Forces. The JSC mission is integral to other vital activities such as Information Operations (IO), Electronic Warfare (EW) and other special projects as directed by the Joint Staff.

This funding will continue EM interference resolution support (analyzing incidents of frequency interference, determining causes, and recommending methods of resolution); deployed operations support as required by COCOMs; exercise support; performance of high frequency (HF) radio propagation predictions for skywave paths; and development of country study reports as requested by the COCOMs.

I. Description of Operations Financed: (continued)

e. Defense Information Systems Network Enterprise Activities (FY 2010: $90,053 thousand): Defense Information System Network (DISN) is DOD's consolidated global telecommunications infrastructure supporting end-to-end information transport for DOD operations. The system provides the warfighters and the COCOMs with a robust Command, Control, Communication, Computers and Intelligence (C4I) information long-haul transport infrastructure. The DISN goal is to span the terrestrial and space strategic and tactical domains for interoperable telecommunications connectivity and value-added services required to plan, implement, and support any operational missions.

The funding (FY 2010: $61,404) continues the sustainment of the DISN of which 47 percent or 28,860 supports the multiyear circuit transition activity. The non-recurring transition costs include planning and integration, contractor labor, minor equipment, installation, circuit dual operations, travel, and testing to ensure uninterrupted customer service through all circuit transitions. Transition funding also supports the product support planning reviews needed to accomplish integrated planning for technical refresh implementation and monitor accomplishments against the scheduled activities. The Access Transition Initiative (ATI) circuits must be transitioned from expiring contracts to either the new DISN Access Transport Services (DATS) contracts, GSA's NETWORX contract or onto the DISN Core and the DISN Transmission Services - Pacific (DTS-P) project. Specific goals include moving the remaining 1465 circuits from the DISN Transmission Services – CONUS – Access Optimization (DTS-C/A/O) contract to DATS contract and 2,336 circuits from the DISN Transmission Services – CONUS Extension (DTS-CE) to DATS contract. In addition, 26 percent or $15,965 of this funding pays for: DISN bandwidth in Kosovo; Defense Satellite Communications System (DSCS); and Enhanced Pentagon Capability (EPC)/Survivable Emergency Conferencing Network (SECN). Kosovo funds reimburse circuit costs incurred in the Defense Working Capital Fund. DSCS and EPC/SECN costs are comprised of technical assistance, depot support, maintenance, licenses, program support,

I. Description of Operations Financed: (continued)

performance analysis, and circuit engineering. Last, 27 percent or $16,579 of the FY 2010 funding provides for pay, benefits, and program support for DSCS and Senior National Leadership Communications plus management support activities to include quality assurance, logistics, and applications sustainment.

The funding ($3,465 thousand), will be used to enhance the operational effectiveness and efficiency of the services and capabilities to include Information Assurance (IA) measures (required by the National and DoD Space Policy for COMSATCOM supported DoD missions); service portability, flexibility, and optimization; faster provisioning responsiveness to support urgent requirements; greater use of DoD Teleports; broader geographic coverage; increased protection and capacity; network operations monitoring and fault reporting: improve performance management; improve overall customer satisfaction and quality of service; and develop the future COMSATCOM services acquisition to support the long-term joint war-fighting Commercial SATCOM Communications services requirements.

Additionally, funding supports Global Broadcast Services (GBS). The GBS is a broadband worldwide SATCOM Service providing high capacity, video, imagery, and data products required to support joint military forces throughout the globe. The DISA supports integration of GBS with the DISN to allow transport (linking Terrestrial and SATCOM) by broadcasting large data files and full motion video from source to tactical end user. Efforts include engineering to support GBS use of WGS satellites, additional integration with DoD gateway locations, full Internet Protocol integration with the DISN core, and development of Satellite Broadcast Management (SBM) failover and traffic rerouting capabilities (GBS COOP). The DISA continues to assist GBS JPO in architecture planning for migration of GBS bandwidth management functions to the Defense Enterprise Computing Centers (DECCs), and facilitate coordination with DISA Computing Services Directorate.

I. Description of Operations Financed: (continued)

The last component of DISN activities is the Systems Engineer for Satellite Communications (SES). The SES is the DoD focal point for SATCOM systems architectural engineering. The DISA supports the Executive Agent (EA) for Space in developing and maintaining the overall DoD SATCOM roadmap. The SES develops from mid and long-term overarching SATCOM architectural recommendations, the specific "Systems of Systems" (SoS) concepts and recommendations for the midterm that can be turned into and/or mapped to specific requirements and capabilities documents for SATCOM systems.
Existing tasks that will be supported by FY 2010 funding, $25,184 thousand:

- Maintain the Satellite Database – the single validated and recognized SATCOM requirements repository
- SATCOM requirements, systems analysis and studies – future SATCOM capability, needs, shortfalls of SATCOM support to operational plans, war plans, scenarios
- Transformational communications architecture – incorporating SATCOM into the overall GIG operations, network operations, situational awareness, network control
- Wideband Global Satellite (WGS) transition - OASD NII and USSTRATCOM tasked DISA to plan the transition and determine costs and schedules of Defense Satellite Communications Systems (DSCS), Global Broadcast System (GBS), and commercial SATCOM users to WGS. Potential cost avoidance of $650M from $1.5B SATCOM lease costs
- Realign the world-wide SATCOM gateway terminals for operations with both DSCS and WGS and identify potential cost avoidance, CONOPS improvements
- Demand Assigned Multiple Access-Compatible (DAMA-C) waveform development and implementation – complete DAMA-C specifications and develop DAMA-C controller for Combat Identification and rescue missions
- Mobile User Objective System (MUOS) end-to-end system engineering – address USD AT&L direction to conduct MUOS end-to-end systems engineering supporting OASD NII

I. Description of Operations Financed: (continued)

f. Defense Information Systems Network Subscription (FY 2010: $13,902 thousand): Enterprise Activities and Subscription Payments is the DoD's consolidated worldwide telecommunications infrastructure that provides end-to-end information transport for DoD operations, providing the warfighters and the Combatant Commanders with a robust Command, Control, Communications, Computers and Intelligence (C4I) information transport infrastructure. The DISN continues to evolve to meet DoD requirements including Mobile Satellite Services (MSS), DISN-Global Broadcast Services Integration (GBS), National Command Authority (NCA) Conferencing Enhancement Project (NCEP) and the GIG-CS, each has added specific activities/requirements. The DISN goal is to span the tactical, terrestrial and space strategic domains seamlessly, to provide the interoperable telecommunications connectivity and value-added services required to plan, implement, and support any operational mission. Driven by both evolving technology, and rapidly increasing customer requirements, the DISN is undergoing a transformation process in two forms: first, technological transformation-driving initiatives such as GIG-CS and the DISN Next Generation (DISN NG) replacement acquisition contracts and, second, the business transformation process implemented through the DoD Enterprise Communications assessments.

I. Description of Operations Financed: (continued)

3. GIG Network Operations and Defense:

Mission Area Component ($ in Thousands)	FY 2008	FY 2009	FY 2010
a. Network Operations	9,984	17,277	21,285
b. Info Systems Security Program/Info Assurance/PKI	217,709	313,031	314,032
c. Comprehensive National Cybersecurity Initiative	0	32,493	63,598
d. Field Commands and Field Offices	61,136	48,085	61,603
e. Joint Staff Support Center	22,572	24,556	28,343
f. Defense Industrial Base	0	1,994	4,925
g. JTF-GNO	13,213	181	18,863
GIG Network Operations and Defense Total	**324,614**	**437,617**	**512,649**

a. Network Operations (FY 2010: $21,285 thousand): Network Operations (NetOps) provides the operations, integration and synchronization of the Agency's 4 Theater Network Operations Centers (TNCs), the Global NetOps Support Center (GNSC), 16 DoD SATCOM Gateways, and 9 COCOMs Global/Joint Theater NetOps Coordination Centers Capabilities transformation initiatives to ensure timely capabilities improvements, improved efficiencies and business practices, end-to-end interoperability and reliable/secure operations. Due to growing demand for IP-over-SATCOM capabilities at DoD SATCOM Gateways, additional resources are required for both contractor and civilian, to deploy and support the already existing contracted workforce at Theater NetOps Centers. The mission demand grew from 300 missions per year to over 350.

The funding supports the following key integration and synchronization actions:

I. Description of Operations Financed: (continued)

- Integrate and synchronize GIG NetOps transformation initiatives focused on TNC enablers providing improved effectiveness and efficiencies internally and vertically
- 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
- Transform DISA Network Operations, promote shared situational awareness and synchronize the operations of 11 Major Network, Enterprise, and Computing Services NetOps Centers through the NetVision efforts
- Prepare, test, manage, and execute the Agency's Continuity of Operations Plan (COOP)
- Establish the DISA's Information Technology Infrastructure Library (ITIL) Framework
- Maintain a Network Operations (NetOps) readiness review process that ensures DISA products and services are manageable and sustainable throughout the lifecycles
- Furnishes knowledge management support to the field via a variety of venues such as VTC, e-Collaboration, and information repositories
- Provide agency oversight and representation on the Defense Information Assurance Security Accreditation Working Group (DSAWG)

Theater and Global NetOps Centers coordinate the DISA and JTF-GNO response actions to NetOps events across the entire GIG, end to end and non-DoD interfaces:

I. Description of Operations Financed: (continued)

- Provides operational direction and control to, and maintains status of 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 for integrity of the GIG
- Exercise operational direction of the Defense Satellite Communication System (DSCS) Enterprise/Gateway terminals and DSCS space segments through the Joint Task Force - Global Network Operations (JTF-GNO) Global Satellite Support Center (GSSC), Theater NetOps Centers (TNCs), and the Wideband Satellite Operations Centers (WSOCs). As the Gateway Consolidated SATCOM System Expert ensure the integration of DoD Gateway, Teleport, and STEP SATCOM Capabilities into the GIG.
- Manage the DoD MILSATCOM satellite terminal and modem certification programs in support of DISA's Joint Staff assigned role as the System Engineer for SATCOM

This effort includes funding contractor support to transition from commercial satellites to government satellite systems, and deployments to austere locations where commercial terrestrial services are not mature enough to provide a robust communications network, Network Operations management of equipment, and networks for the front line and rear echelon warfighter. This funding will significantly enhance management and control capabilities of existing NetOps organizations to fully support the warfighter.
Specific capabilities starting in FY 2010 include:

- Providing technical direction and oversight for IP asset network management, mission planning, equipment configuration, and pass-phrase distribution for IP modems and associated IP-over-SATCOM equipment at DoD SATCOM Gateways

I. Description of Operations Financed: (continued)

- Providing technical direction and oversight for Tier 1/2 incident management and Tier 3 engineering, problem resolution, and configuration management for IP modems and convergence equipment at SATCOM Gateways
- Development of Agency and DoD strategy for evolution of DoD SATCOM Gateways while representing the operational community of interest in the development of Enterprise Architectures for SATCOM and Gateway capabilities
- Performing trend analysis of DoD SATCOM Gateway performance and utilization, making recommendations to the Agency, Joint Staff, and DoD regarding capability sustainment, enhancement, modernization, or retirement
- Conducting cross-program coordination and synchronization between the Armed Services, Combatant Commands, and Defense Agencies
- Developing policies and procedures for operational use of DoD Gateways, resolve operational and procedural issues, coordinate with incident managers to identify and resolve systemic problems, and coordinate configuration management activities at DoD Gateways to ensure service availability to deployed users
- Providing technical direction and oversight for IP asset network management, mission, planning, equipment configuration, and pass-phrase distribution for IP modems and associated IP-over-SATCOM equipment at DoD SATCOM Gateways

This funding also supports the GIG Customizable Operational Picture (GIGCOP), which provides a comprehensive, integrated, end-to-end Situational Awareness (SA) view of the GIG to Network Operations (NetOps) personnel. This capability expands SA beyond current enclave-level views to GIG-wide situational awareness by integrating and correlating events from cross-enclave data sources. The NetOps personnel can customize multiple GIGCOP tools and dashboards to filter and categorize data collected from numerous NetOps data sources on the GIG. The customizable filters and tools allow users to monitor near

I. Description of Operations Financed: (continued)

real-time correlated data from several sources and review its relevance for identifying and addressing malfunctions and malicious activity on the GIG.

b. Information Systems Security Program (ISSP)/Information Assurance (IA)/PKI (PKI): (FY 2010: $314,032 thousand): The DISA's Information Systems Security Program (ISSP) ($273,449 thousand), is comprised of numerous DoD-wide efforts to manage information security risks and ensure confidentiality, integrity, authentication, availability, and non-repudiation of users' access to DoD's GIG, a worldwide network, used by the Secretary of Defense, Combatant Commands (COCOMs), Joint/combined task forces, Services, and Agencies for continuous communication between decision-makers and warfighters. The DISA employs a defense-in-depth strategy with layered protections (perimeter and host/enclave), assured information sharing, global situational awareness (including attack detection and diagnosis) of the GIG, and numerous cross-cutting foundational initiatives (portal, training, standards and guidelines, security reviews). The DISA's ISSP funds continued deployment and sustainment of numerous capabilities needed to close cyber security gaps that adversaries are currently exploiting and using to compromise critical missions at home and abroad. The program will increase the number of civilian FTEs by 135 starting in FY 2010.

To maintain the security of the GIG perimeter, the Demilitarized Zone (DMZ) architecture will implement enterprise level capabilities that protect against dangerous protocols, secure Domain Name Systems (DNS) and secure enterprise wide support to the teleworking force. The DISA is working to update policies for the DNS security, maintain 100 percent up-to-date patches for the DoD community, and provide DNS situational awareness on the NIPRNET. The DISA is migrating applications within the DMZ Extensions in order to protect private or controlled data by implementing data segregation from publicly accessible information. In addition, DISA will implement email and web traffic

I. Description of Operations Financed: (continued)

filtering between NIPRNet and the Internet and improve security within the DMZs. The DISA is expanding network mapping capabilities used on SIPRNet to NIPRNet.

Host/Enclave initiatives are a fundamental component of an integrated defense-in-depth strategy. The DISA's initiatives improve active protection of individual hosts and servers, enhance system administrators' ability to identify and mitigate variances in systems' configuration management, and manage access between an enclave boundary and networks. In FY 2010, policy enforcement prior to a system being connected to the network will be controlled and tools are available to detect and analyze suspicious insider activity.

The Host-Based Security Service (HBSS) is a suite of "on-board", policy-based defensive measures that constrain the operation of software running on a system to pre-defined, acceptable behaviors. The HBSS will implement the deployment of standard configuration management policies and the ability to view host-level trends and patterns.

In FY 2010, DISA will continue to provide enterprise licenses for antivirus/antispyware tools which detect and eradicate viruses and other malware on over 4 million DoD hosts. The Assured Compliance Assessment Solution (ACAS) (formerly Secure Configuration Compliance Verification Initiative (SCCVI)) efforts provide external scanning of systems. This enhanced enterprise level tool will generate cost savings across the DoD by eliminating individual service contracts.

A primary effort of the Department is Insider Threat capabilities directly address one of the most potentially devastating threats to DoD networks--malicious insiders or adversaries who are able to masquerade as credentialed insiders. This initiative

I. Description of Operations Financed: (continued)

eliminates the piecemeal and limited approach to detecting, analyzing, and confirming insider threat activities that the Department has today.

The DISA plays a critical role in implementing the Enterprise Cross Domain Service (CDS) to enable warfighters and DoD users to safely and securely share information between networks of different security levels. The enterprise CDS effort allows increased dissemination of information among users while decreasing costs. In FY 2010, DISA will sustain three CDS sites (2 CONUS, 1 OCONUS) and customers. The DISA will also implement new capabilities for secure transmission of MS Office files from NIPRNet to SIPRNet.

The DISA increases the Situational Awareness (SA) of the Information Assurance (IA) and network management postures of the DoD network by deploying and sustaining the Computer Network Defense User Defined Operation Picture (CND UDOP) and GIG Customizable Operational Picture (GIGCOP) tools. In FY 2010, DISA will transition to an integrated capability for GIG SA to include a collaborative environment that enables users to post, edit, and search incident data based on the NetOps data strategy.

The DISA's Attack Detection and Diagnosis Initiatives include incident handling repositories, sensors, and Security Information Managers (SIMs). The DISA maintains a set of enterprise repositories – Joint Computer Emergency Response Team (CERT) Database, Joint Threat Incident Database, DoD CERT Incident Database - that are the core of the DoD's global view of all reported incidents and events occurring on DoD networks. These enterprise repositories allow CC/S/A intel analysts to share, enter, query and track DoD IA incident/event/threat data and generate reports via the web. The information maintained within the repositories, combined with the data correlation capabilities, enable Intel analysts to correlate threat and threat entity data with specific incidents

I. Description of Operations Financed: (continued)

to develop and analyze problem sets, and allow analysts to make long and short-range predictions of threat intentions and capabilities.

The DISA operates and expands several sensing appliance tools for network traffic analysis, signature detection, and full-packet capture at routers (connection points) that makeup the NIPRNET and SIPRNET backbones. These sensors will work against current and emerging threats to the GIG by supporting detection and remediation of attacks. In FY 2010, DISA will maintain the 517 previous deployed sensors and continue purchasing approximately 240 sensors for the DoD community.

Cross-cutting foundational IA products and services include the IA portal, IA training for development of the IA workforce, IA standards and guidelines, automated security software update services to address system vulnerabilities, security assessments, compliance visits, and onsite IA support at 11 Combatant Commands. The DISA maintains an IA Portal for disseminating IA policy and strategies via links to resources, policy, training, and a working group collaborative tool. The FY 2010 funds support development of four new training packages and dissemination of over 22,000 packages yearly. The DISA will expand computer-based training on SIPRNet. The DISA establishes/maintains the Security Technical Implementation Guides (STIGS) that define IA configuration standards and provide guidance to assure system confidentiality, integrity, and availability while maintaining a balance operational capability and flexibility. The FY 2010 funding will provide for at least five new STIGs and checklists to address emerging threats to the DoD network. The DISA provides an automated mechanism for distributing and installing critical updates on the SIPRNET and NIPRNET; in FY 2010, an expected 120,000 downloads of security software will be accessed from these systems. Equipment that is properly patched and protected decreases the probability of adversarial attack success and increase attack detection rates. Sustainment of a Certification and Accreditation (C&A)

I. Description of Operations Financed: (continued)

automated system reduces the time and cost to certify and accredit systems. The DISA will continue conducting over 65 examinations a year. The DISA has implemented more in-depth Enhanced Compliance Validations (ECV) reviews which evaluate a site's current network configuration and security readiness. The DISA will conduct approximately 130 ECV reviews at DoD's most critical sites each year beginning in FY 2010.

The DISA facilitates sharing of information under the Joint Enterprise Directory System (JEDS) that compiles user contact information and identify attribute repositories in one location so that users of the SIPRNET and NIPRNET can facilitate net-centric sharing of information. In FY 2010, DISA will provide upgrades to deployed JEDS capabilities.

The GIG Operations is responsible for the defense-in-depth approach to Information Assurance (IA), certification and incident detection and resolution. These areas are covered under programs such as: Sensor Grid Operations, the Computer Emergency Response Team Coordination Center (CERT/CC), Computer Network Defense Service Provider (CNDSP), Theater NetOps Center–Net Defense Branch (TNC-ND), and Mission Assurance Support Capability (MASC). MASC personnel serve as liaisons between the COCOMs and the TNC/GNSC functions and provide the COCOM NOSC watch officer with situational awareness on ASIs, outages, implementations, and emerging technologies.

Current network operations and defense funding supports many key Information Assurance (IA), readiness reviews, and detection positions. Since DISA provides backbone communications to the war-fighter, analysis of threats and recovery from incidents to the DoD networks is critical to the COCOMs, GNSC/TNCs, and JTF-GNO communication situational awareness of the GIG.

I. Description of Operations Financed: (continued)

The major decreases in the FY 2010 funding request of $25,696 include:

- -$11,065 thousand: JTF-GNO internal realignment of funds within GIG Operations.
- -$ 4,000 thousand: Movement of O&M to MILCON funding.
- -$757 thousand: Reduction of technical support in the Contract Advisory and Assistance Services (CAAS).

The Department of Defense (DoD) PKI is the mechanism that provides public key certificates to support DoD mission critical applications. The PKI supports the infrastructure for the entire DoD and is a key component in enabling information sharing in a secured environment. The PKI will provide a framework for secure information sharing with external partners. This framework operates to support the Department's IA requirements for confidentiality, authentication and identification, verifying data integrity, non-repudiation of communications or transactions, and digital signatures. The PKI is available on both the NIPRNET and SIPRNET providing support to 4.1M Common Access Card (CAC) NIPRNET users and 45,000 SIPRNET users. Currently, over 95 percent of DoD website servers utilize DoD PKI and ultimately all DoD applications and web sites on NIPR and SIPR will utilize PKI. The PKI will continue to evolve to accommodate the Presidential Directive for a Common Electronic Credential Identification Standard for Federal Employees and Contractors.

The National Security Agency (NSA) is the PKI Program Manager, and provides funds for the engineering and sustainment support of 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. The DISA Information Assurance and PKI provide for system upgrades, implementation, operations and sustainment, registration authorities training, interoperability testing, procurement of equipment, along with software and hardware acquisition and maintenance for the DoD PKI.

I. Description of Operations Financed: (continued)

DoD PKI protects information by safeguarding data as it is being created, used, modified, stored, moved, and destroyed, on the communication networks, within the enclave, at the enclave boundary, at the client, and within the computing environment to ensure that all information has a level of trust commensurate with mission needs.

The FY 2010 funding, $13,171 thousand, will be used to operate and sustain the DoD PKI (including hosting in secure computing facilities, robust help desk support, operational monitoring and auditing), implement system upgrades (including performance of interoperability and operational testing), provide training for registration authorities and users, and provide public key enablement consultation.

c. Comprehensive National Cybersecurity Initiative (FY 2010: $63,598 thousand): The program is performing classified work. Detailed information is submitted separately in classified Department of Defense exhibits.

d. Field Commands and Field Offices (FY 2010: $61,603 thousand): The DISA's four Field Commands and seven Field Offices, with 29 locations in 7 countries, are forward deployed and co-located with the Combatant Commands. The DISA Field Commands and Offices serve as the DISA Director's forward direct support element to the Combatant Commanders/Component Commanders (COCOMs) for all DISA services, new capabilities policy, and planning. Funding provides for security that contributes to the deterrence and warfighting mission while laying groundwork for introduction of DISA systems and upgrades. The DISA's Global Network Support Center (GNSC), under operational control of USSTRATCOM, exercises centralized management of CONUS network operations and is responsible for the real-time operational direction, monitoring and control of the DISN networks within CONUS.

I. Description of Operations Financed: (continued)

The Field Commands requirements are increasing due to additional support demands from the COCOMs for global presence and mission areas.

Major items increasing program growth for FY 2010 include:

- +$1.53M: The standup of the DISA USAFRICOM Field Office in Germany
- +$4,600: Agency realignment caused increases in payroll costs
- +$1,210: Base operations support at DISA PACIFIC, DISA CENTCOM, and DISA SOUTHCOM locations
- -$413: Reduction of technical support in Contract Advisory and Assistance Services (CAAS)

These increases are due to increasing growth and demands on the DISN infrastructure and NetOps supported by DISA. The Base Operations Support (BOS) will provide the resources necessary to operate the DISA facilities. These resources sustain mission capability, quality-of-life, work force productivity, and fund personnel and infrastructure support. The higher demand and constant growth has caused some field locations to be operating at maximum building capacity. The DISA has submitted a FY 2010 Military Construction request to expand facilities and building upgrades.

e. Joint Staff Support Center (JSSC) (FY 2010: $28,343 thousand): The JSSC directly supports the Joint Staff by conducting 24x7 watch/monitor operations in the National Military Command Center (NMCC) for C4I systems, strategic threat operational warning, and local Global Command and Control System (GCCS-J) - Joint operations maintenance. The JSSC provides the 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,

I. Description of Operations Financed: (continued)

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.

f. Defense Industrial Base: (FY 2010: $4,925 thousand): The program is performing classified work. Detailed information for this program is submitted separately in classified DoD exhibits.

g. Joint Task Force-Global Network Operations (JTF-GNO) (FY 2010: $18,863 thousand): Joint Task Force – Global Network Operations (JTF-GNO) directs the operation and defense of the GIG to enable timely and secure net-centric capabilities across strategic, operational, and tactical boundaries. The JTF is a unique capability that operates at the boundary between operational customers and enterprise communications and security providers. The 24x7 operations support a full spectrum of war fighting, intelligence, and business missions that includes a surge capability for enhanced customer support to global operations in times of crisis. To fulfill its mission the JTF takes a number of measures to both defend the GIG and assure the continuity and quality of Defense communications. Funding levels support the following mission elements:

- Supports GIG information security with proactive coordination and response through the identification and mitigation of threats and extensive analysis of network events, ongoing intelligence analysis, and immediate response to, and mitigations of, current attacks.
- Manages scheduled and unscheduled GIG outages and formal/operational liaison with a growing set of mission partners at federal, commercial, and international levels.

I. Description of Operations Financed: (continued)

- Provides the White House, congressional leadership, and DoD senior leadership technical and functional review of policy, position papers, reports, proposals, and any other Network Operations related issues. Additionally, it chairs the Network Operations Community of Interest for the Department and provides the leadership necessary to enable the GIG's move to NetCentric operations.

An internal realignment starting in FY 2010, places current JTF-GNO resources in its own unique product line in pay and non-pay. This funding will support:

- Providing timely threat characterization, attribution, and Indications and Warnings (I&W) would lead to:
  - the denial of services at the Internet Access Points and/or delays implementing corrective and mitigating actions
  - identifying intruders having the ability to operate virtually undetected in DoD networks for long periods of time, exfiltrating data, and expanding their footprint in DoD networks.
- Defining operations and requirements for key cyber initiatives by supporting the development of joint cyber space operation concepts, plans, and orders

I. Description of Operations Financed: (continued)

4. Exploit the GIG for Improved Decision Making:

Mission Area Component ($ in Thousands)	FY 2008	FY 2009	FY 2010
a. Global Command and Control System-Joint	80,915	88,570	66,670
b. Global Combat Support System	15,512	17,843	16,195
c. National Military Command System	2,587	6,966	4,475
d. Senior Leadership Enterprise	0	0	55,924
e. Defense Message System	11,398	16,195	14,329
f. Combined Enterprise Regional Information Exchange System	33,092	39,870	44,136
g. Net-Enabled Command Capability	14,813	10,893	9,602
h. Electronic Commerce	48	13,745	0
i. Other Programs	13,561	13,279	14,708
Exploit the GIG for Improved Decision Making Total	**171,926**	**207,361**	**226,039**

a. Global Command and Control System-Joint: (FY 2010: $66,670 thousand): The Global Command and Control System-Joint (GCCS-J) is the DoD joint Command and Control (C2) system of record for achieving full spectrum dominance. The 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, National Military Command Center, Combatant Commanders, Joint Force Commanders, and Service Component Commanders. Employing the DISN, GCCS-J offers vital connectivity to the systems the

I. Description of Operations Financed: (continued)

joint war fighter uses to plan, execute, and manage military operations. GCCS-J is a major IT investment and is designated an Acquisition Category IAM Major Automated Information System (MAIS) program. The GCCS-J is being implemented in an evolutionary manner through distinct blocks, using spiral development. Each block is self-contained; targets a specific set of Joint Staff validated, prioritized user requirements, and deliver multiple releases of GCCS-J of record for achieving full spectrum dominance. GCCS-J employs a predominantly open system client/server architecture, which is evolving to a web-based architecture that allows a diverse group of COTS and GOTS software packages to operate at any GCCS-J location. The 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 combatant commands at sites around the world, supporting joint and coalition operations. This effort provides 24x7 global help desk support, via the Joint Staff Support Center (JSSC) and the National Military Command Center. The JSSC is the primary entry point for resolving all operational GCCS-J hardware, software and network issues. 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. The COE sustainment funding aligns with the GCCS-J schedule for release of a non-segmented server/client.

One of the capabilities that will transfer from GCCS-J to NECC is Adaptive Planning (AP). 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) are a suite of software tools that provides AP capabilities to include: campaign planning, forecast predictions, information management and rapid

I. Description of Operations Financed: (continued)

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. CFAST facilitates the dynamic preparation of campaign plans for rapid expeditionary environments to meet DoD planning doctrine requirements of ongoing operations and future contingencies used by the COCOMs. OSD and Joint Staff use CFAST to model how DoD will respond to current and future conflicts using a variety of scenarios for the Operational Analysis missions.

The FY 2010 GCCS-J I3 will increase personnel to support CENTCOM requirements and deployed forces in the Southwest Asia (SWA) Area of Responsibility (AOR). On-site personnel resources will triple, from 12 to 36, to stand-up and operate systems in the forward Operating Bases in Kabul, Bagram, and Kandahar. Funds will sustain and enable access to new Army, NATO, coalition and Intel reporting systems of GALE Lite, CIDNE, and NATO/ISAF.

Those systems enable the U.S. and NATO to share situational awareness of individuals, events, and organizations between Army ASAS-Lite systems and the joint system of record, Global Command and Control System (GCCS) Integrated Imagery and Intelligence (I3). This is in addition to sharing dynamic force tactical dispositions among all participants. The CDS solution will reduce the hardware footprint and process complexities now required for information sharing with coalition partners. Funding will continue maintenance and update other ongoing software enhancements in support of the Stability and Sustainment Operations (SASO) requirements.

The CFAST currently operates and maintains three nodes (Secret, Development, and Training). The Secret Node supports current operations. The Development Node is used to support spiral development and testing of new and enhanced functional capabilities and

I. Description of Operations Financed: (continued)

troubleshooting problems from the field. The Training Node is used to teach Adaptive Planning tactics, techniques, and procedures. CFAST operates the three nodes with a system administration team operating 24x7x365. The system administrators perform Level II and Level III help desk support in addition to monitoring the health and status of the tool suite and addressing software errors and resolving user problems. The system administrators also install the version releases, conduct self-assessments and IAVA compliance in compliance with information assurance regulations, and other network tasks. CFAST also provides resident subject matter experts (SMEs) to educate and train the users currently in the field on the AP process and the use of CFAST software. The SMEs reduce the government's risk by refining user requirements and providing feedback to the user representatives. CFAST has the requirement to provide a Continuing Operations (COOP) Node and a Top Secret Node to meet Joint Staff prioritized and validated requirements.

The FY 2010 funding supports the operations and maintenance (helpdesk, software license renewals, software error correction, IAVA compliance) of the Secret, Development, and Training Nodes. In addition, funds provide operations and maintenance of a COOP Node and a Top Secret Node.

b. Global Combat Support System: (FY 2010: $16,195 thousand): The Global Combat Support System (Combatant Command/Joint Task Force) [GCSS (CC/JTF)] is an initiative that provides end-to-end visibility of retail and unit level Combat Support (CS) capability up through the National Strategic Level facilitating information interoperability across and between CS and Command and Control (C2) functions. The GCSS(CC/JTF) provides decision makers with fused CS data and C2 information on the same workstation. The GCSS (CC/JTF) provides the critical information technology capabilities required to move and sustain joint forces throughout the spectrum of military operations. GCSS (CC/JTF) uses a web-based Portal environment with Single Sign On (SSO) access (PKI / Common Access Card

I. Description of Operations Financed: (continued)

(CAC)) to meet the Focused Logistics tenets and to implement the vision of Network Centric Warfare.

In FY 2010, the Program will continue its transition to a service-oriented architecture (SOA) in a net-centric environment utilizing the Net-Centric Enterprise Services (NCES) core concepts and Business Intelligence, Workflow, Knowledge Management, Web Service Management, and Security tools. The architecture includes implementation of a more robust Continuity of Operations Plan (COOP), Contingency Site, Enterprise System Management (ESM), and security (e.g., intrusion detection on GCSS strategic servers and next generation guards) processes and tools. This robust architecture is the enabler for the Program to become fully net-centric and accelerates the introduction of new data source integration and application development; permits greater flexibility for the joint logistics warfighter in the evaluation and view of fused data; increases dynamic report capability; provides more rapid exposure of data to communities of interest; and enhances the security posture of the system.

Within the GCSS Family of Systems (FoS), DISA is responsible for two main efforts which are the 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 with C2 information to provide the joint warfighter with the ability to plan, execute, monitor, and control logistics operations. The GCSS (CC/JTF) provides applications, decision support tools, and visualization mechanisms to enable the joint logistics warfighter to assess and analyze information to rapidly make critical decisions. The GCSS (CC/JTF) significantly increases access to information stored in multiple databases via a SSO web portal application, using a SIPRNET PKI certificate and for the NIPRNET capability, a CAC. The GCSS (CC/JTF) infrastructure provides secure web-

I. Description of Operations Financed: (continued)

access, discrete user account administration, data mediation, and enterprise management features that facilitate delivery of capabilities meeting the vision of a net-centric architecture to support the warfighter.

The FY 2010 funding is critical to the GCSS Program Management Office's ability to fund Computing Services. Computing Services (SMC-Montgomery and DECC-Pacific) provide the operational support for the GCSS SIPRNet and NIPRNet systems which are used by Combatant Command/Joint Task Force Commanders world-wide and service fielding and maintenance activities associated with software development and integration contract.

c. National Military Command System: (FY 2010: $4,475 thousand): The NMCS provides Senior Leaders, National Military Command Centers (NMCCs), Executive Travel Fleet, Office of the Secretary of Defense (OSD), the Chairman of the 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, maintain situational and operational awareness through crisis action and operational capabilities. 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 customer with 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. 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.

The FY 2010 funding will provide enhanced capabilities for performing configuration management of NMCS assets (particularly C2 systems) and facilities; providing technical

I. Description of Operations Financed: (continued)

assessments and engineering support to modernize and transform the NMCS via technology insertions; implementation of an NMCS enterprise-wide Information Resources Management (IRM) infrastructure; and mirroring of NMCC systems at NMCC Site R and other NMCS nodes.

Additionally, the funding supports NMCS/DNLCC 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. Senior Leadership Enterprise (FY 2010: $55,924 thousand): The program is performing classified work. Detailed information for this program is submitted separately in classified Department of Defense exhibits.

e. Defense Message System (FY 2010: $14,329 thousand): The Defense Message System (DMS) is DOD's "system of record" for the exchange of official record information including directives, policy, decisions, and directions. The DMS provides "command and control" capabilities that support operational missions, while providing formal interoperability with non-DOD activities, such as Homeland Security, State, and the CIA. The DMS supports the U. S. requirement for formal/organizational military messaging capability with NATO, international defense organizations, civil organizations like the Red Cross, and various foreign nations (e.g., the United Kingdom, Canada, Australia, and Japan).

I. Description of Operations Financed: (continued)

FY 2010 funding, $14,329 thousand, will support system engineering and integration; management and oversight of the program's primary sustainment contract; program cost analysis; and milestone management required by the DMS Global Service Manager. Sustainment activities are intended to ensure that DMS COTS-based applications retain compatibility with commercial technical refreshes; correct operational deficiencies; and incorporate security protection against newly identified threats.

f. Combined Enterprise Regional Information Exchange System (FY 2010: $44,136 thousand): The Multinational Information Sharing (MNIS) Program is a portfolio of three coalition information sharing capabilities designed to enable sharing of operational and intelligence information among US forces and multinational partners. The first is the Combined Enterprise Regional Information Exchange System (CENTRIXS) supports intelligence and classified operations and information exchange and sharing at the Secret Releasable (REL) level. There are multiple, cryptographically-isolated CENTRIXS enclaves serving various communities of interest (COI) that support multinational efforts to include Operation Enduring Freedom (OEF), Operation Iraqi Freedom (OIF), the Overseas Contingency Operations (OCO) and counter-narcotics operations. CENTRIXS is regionally focused and COCOM centric. These networks allow the US 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 commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) solutions to reduce implementation costs while providing a robust, innovative approach to warfighting communications. CENTRIXS services include providing common and consistent situational awareness of the battlefield via Common Operational Picture (COP), Common Intelligence Picture (CIP), Intelligence, Surveillance and Reconnaissance (ISR), information and improved information sharing via secure Voice over Internet Protocol

I. Description of Operations Financed: (continued)

(VoIP) telephony, Web Services, email with attachments, and other information services supporting coalition operations.

The DISA-provided services include Active Directory, Domain Name Service (DNS), Network Time Protocol Services, Windows Software Update Service (WSUS), anti-virus definitions, CENTRIXS Central web services, Google Search and Google Earth, Microsoft Exchange for Combat Support Organizations, Voice-Over Internet Protocol (VoIP), and email.

The MNIS is supporting COCOMs through site surveys, network design, purchasing equipment, developing, expanding, repairing existing networks, and training on-site COCOM personnel. The PMO supported the repair of the Pakistan Army CENTRIXS GCTF circuit and familiarizing incoming engineers to facilitate communication between the US / International Security Assistance Force (ISAF) and Pakistan (PAK) Army personnel Engineers are working with NAVCENT in Bahrain to bring a subset of the GCTF/CMFC network into the Iraq Area of Responsibility (AOR). This funding will sustain the CENTRIXS-enhanced footprint and enable continued coalition information sharing in support of the aforementioned multinational efforts. The DISA will field capability to satisfy the Net-Centric Functional Capability Board (NC FCB) approved CENTRIXS Cross Enclave Requirement (CCER). CCER is a pre-planned product improvement that will use COTS products to converge multiple cryptographically isolated CENTRIXS networks into a single warfighting information sharing environment. When implemented, CCER will satisfy COCOM coalition information sharing requirements while reducing infrastructure footprint and sustainment costs. Additionally funding will enable the sustainment of the cmil.mil architecture build-out that will provide Global IP Transport for the CCER capability and be used to maintain VPN management, the fielded DoD PKI and the network monitoring required to provide the data integrity, user identification and authentication, and data

I. Description of Operations Financed: (continued)

confidentiality for the CCER environment, and support the engineering services to maintain the CCER architecture.

The second MNIS portfolio member is Griffin which interconnects the national C2 systems of Combined Communications Electronics Board (CCEB) Nations, to include Australia, Canada, New Zealand, United Kingdom and the United States, using Cross Domain Solutions (CDS) that enable information sharing to facilitate situational awareness and operational planning/execution. Current services include cross-domain email with attachments and the United States-United Kingdom (US-UK) Blue Force Track feed. Services are provided from Defense Enterprise Computer Center (DECC)-Pacific and the primary operational node at a contractor facility in the National Capital Region (NCR). The Improved Connectivity Initiative (ICI) is a 5-phase effort to transition the high assurance guard-based interfaces to COTS security appliances. Transitioning to COTS-based interfaces will enable the rapid introduction of a richer set of services among the CCEB nations as current high assurance guard products only satisfy a small number of the overall information sharing requirements. Initial efforts are focused on email services with Australia and will expand to other services and CCEB nations as the proof of concept is achieved. In FY 2010, additional services will be provided using CDS and COTS security appliances as appropriate.

Implementation of Griffin at DECC-Columbus will complete the initial centralized services efforts. The FY 2010 funding will be used for CENTRIXS (to include CCER) and Griffin (to include ICI) hosting and associated NetOps (i.e., network management, Virtual Private Network (VPN) management and Information Assurance/Computer network Defense (IA/CND) services, to centralize additional coalition information sharing enterprise services. Currently there are no reimbursable or DISN Subscription Services (DSS) for the operational coalition environment enterprise services.

I. Description of Operations Financed: (continued)

The final MNIS portfolio member is the Combined Federated Battle Laboratory Network (CFBLNet) which provides a controlled Research, Development, Trials and Assessment (RDT&A) coalition information sharing "sandbox." This sandbox will evaluate new technologies, develop tactics, techniques and procedures that facilitate the transition of promising technologies and capabilities into operational multinational information sharing capability enhancements. The CFBLNet initiatives also support the development and refinement of tactics, techniques and procedures prior to operational deployment. Key initiatives support ISR, missile defense, and NATO force inter-operability testing.

The FY 2010 funding increase will install support network and data storage equipment; centralized data centers and enterprise services support; establish a centralized coalition NETOPS; and implement a global architecture supporting COCOM coalition information sharing not reliant on Cross Domain Solutions.

g. Net-Enabled Command Capability (FY 2010: $9,602 thousand): The Net-Enabled Command Capability (NECC) is the DoD's principal joint command and control capability focused on providing the Warfighter with the data and information needed to make timely, effective and informed decisions. Commanders use NECC to adapt rapidly to changing mission needs by defining and tailoring information environments and drawing on capabilities that enable the efficient, timely and effective command of forces and control of engagements. NECC provides the DoD with next-generation Command and Control (C2) capabilities using a Service Oriented Architecture (SOA) on the GIG. The NECC draws from the C2 community to evolve current and provFide new C2 capabilities into a fully integrated, interoperable, collaborative Joint solution. The NECC replaces the GCCS Family of Systems (FoS) with a single joint C2 architecture and capabilities-based implementation that enables advanced distributive, collaborative information sharing vertically and horizontally. The NECC

I. Description of Operations Financed: (continued)

provides additional critical C2 functionality not present today, and establishes the C2 SOA foundation for future net-centric C2 capabilities.

The FY 2010 funding will support hosting of NECC interim CMs to the EGCNs and the DECC, maintaining the 14 CMs developed in previous fiscal years, hardware maintenance, software license maintenance, and the NECC Joint Technical Operations Control Capability (JTOCC). The NECC JTOCC is net-centric with its capabilities provided by participants accessing the JTOCC via the GIG. The JTOCC acts as the primary interface to the Joint Task Force – Global Network Operations (JTF-GNO) operations support for issues relating to the GIG network access and performance. As NECC develops and prepares for fielding spirals of CMs within the development period, additional capacity at the EGCNs will be procured. Additionally, NECC will realize increasing software maintenance costs supporting CM spirals developed in FY 2008 and 2009.

h. Electronic Commerce (FY 2010: $0 thousand): A one time funding request in FY 2009 supported DISA computer hosting costs. No funding is being requested for FY 2010.

5. Deliver Capabilities Effectively and Efficiently/Shared Services:

Mission Area Component ($ in Thousands)	FY 2008	FY 2009	FY 2010
a. Management Headquarters	37,003	36,066	34,142
b. Pentagon Reservation Maintenance Revolving Fund	11,000	14,949	16,167
c. Shared Service Units /Program Executive Offices	38,707	18,825	35,244
d. Other Programs	15,454	119	834
Deliver Capabilities Effectively/Efficiently and Shared Services Total	**102,164**	**69,959**	**86,387**

I. Description of Operations Financed: (continued)

a. Management Headquarters (FY 2010: $34,142 thousand): Management Headquarters is responsible for overseeing, directing, and controlling DISA activities. The staff supports the DISA Director in decision-making, strategy-development, and communicates that information both internally and externally. The staff oversees the acquisition lifecycle management across the agency and ensures compliance with all DoD acquisition policies and mandates. Additionally, funds are used to develop and implement plans, programs and oversight worldwide in the areas of civilian personnel, military personnel, human resource development, organization and manpower program administration, payroll, travel, transportation, mail management, visual information, security, real estate facilities, and supply services. The staff supports DISA's role as a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve DoD.

The FY 2010 net changes result from increases in performance management contract services support, training strategies, travel, printing, and equipment requirements. A DISA initiative resulted in a realignment of civilian payroll and process improvements to more accurately report civilian payroll costs for each DISA program.

b. Pentagon Reservation Maintenance Revolving Fund (PRMRF) (FY 2010: $16,167 thousand): This requirement supports funding for space, services, protection, maintenance, construction, repairs, alterations, or facilities provided at the Pentagon Reservation. The funds will support normal rent costs normally and the following areas of operation:

- Tenant charges and real property operations for Site R which is the alternate command and control location and capability for the DoD if the Pentagon is attacked or unable to carry out all functions; and

I. Description of Operations Financed: (continued)

- 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; Pentagon Force Protection Agency (PFPA) support of PRMRF.

c. Shared Service Units (SSU)/Program Executive Offices (PEO): (FY 2010: $35,244 thousand): The SSU resources are allocated across the products and services contained in the business and mission activities. The model allocates funds using four primary costs 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.

The SSU provides support for finance, manpower/personnel, security, facilities, acquisition, and information technology necessary for agency operations. The SSU ensures compliance with applicable internal controls, operating statutes/regulations, payment of salaries and benefits, and maintenance/sustainment of facilities.

- Chief Financial Executive: Provides financial services automation support to the Agency for the annual Agency-wide financial statements. Conducts economic analyses, cost estimating, and program and organizational assessments. A major challenge is to provide accurate, reliable, and timely financial information in a cost-effective way to support planning, engineering, acquiring, and fielding net-centric solutions and operating the GIG. The FY 2010 funding supports salaries, operating expenses, financial services payables, Balanced Scorecard metrics, and continued implementation of the Defense Agency Initiative (DAI).

I. Description of Operations Financed: (continued)

- Component Acquisition Executive (CAE): Provides acquisition leadership for the implementation of DoD's net-centric vision through the provision of tailored acquisition policies, processes, procedures, tools, lifecycle oversight and a qualified acquisition workforce. Funding supports salaries, operating expenses, training, acquisition workforce development, and certifications.
- Manpower, Personnel and Security (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, travel, transportation, mail management, visual information, security, real estate facilities, and supply services. Funding supports contract efforts for DISA personnel supporting Strategic Management of Human Capital, Manpower Staffing Standards Studies, operations of the DISA Headquarters Compound, operations at the National Capital Region leased facilities and lease rents with GSA.
- Chief Information Officer and Strategic Planning Directorate (CIO): Directs IT policy development and promulgation in DISA and provides Agency oversight for IT systems. The CIO serves as the Agency lead for performance and results-based management, budget and performance integration, strategy execution, and management of strategic customer requirements. The CIO is developing enterprise architecture and serves as the senior decision authority for DISA internal systems; implementing portfolio management; overseeing records management; privacy act management; Clinger-Cohen compliance; providing information assurance support to include the accreditation of DISA information systems; and leads DISA Cross Domain Solutions and DOD/DISA Ports, Protocols and Services Management implementation. The CIO is responsible for leading, advising, and facilitating the transformation of DISA into a knowledge-enabled, process-oriented, and customer-focused organization. Primary program focus is the continued operation and maintenance of the DISA Intranet

I. Description of Operations Financed: (continued)

Services and DISA DKO activities. This office administers the Information Assurance system certification, accreditation, and training.

- PEO-SATCOM, Teleport, & Services (PEO-STS) (FY 2010: $1,040 thousand): PEO-STS is responsible for acquisition oversight of the program management offices for DoD Teleport, Joint IP Modem (JIPM), Commercial Satellite Communications (SATCOM) and other Services. The PEO-STS is responsible for acquisition oversight for the Presidential Communications Modernization Program Office. The PEO-STS's funding provides expert professional contracted support to complement the PEO-STS government staff, in addition to other operational support requirements. The FY 2010 increase will supports the acquisition oversight.

6. Special Missions: The DISA Charter tasks the organization to plan, develop, and support 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.

Mission Area Component ($ in Thousands)	FY 2008	FY 2009	FY 2010
a. White House Communications Agency	125,293	129,723	125,915
b. White House Situation Support Staff	7,585	6,023	6,302
c. Crisis Management System	10,196	9,597	10,018
d. Minimum Essential Emergency Communications Network	7,941	7,963	5,575
e. Communications Management Control Activity	2,867	904	1,310
Special Mission Area Total	**153,882**	**154,210**	**149,120**

I. Description of Operations Financed: (continued)

a. White House Communications Agency (WHCA) (FY 2010: $125,915 thousand): The White House Communications Agency (WHCA) is a joint service military agency under operational control of the White House Military Office (WHMO) and administrative control of DISA. The WHCA funding supports operations and maintenance of equipment, facilities and personnel 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 National Security Council (NSC), WHMO, and others. Also, the WHCA's provides funding to operate both the fixed and travel communications mission, such as:

- Presidential and Vice Presidential trip support, with historical operational tempo average is 624 missions per year.
- Life cycle replacement, replenishment, technical refresh, and sustainment costs for maintaining communications support for the White House.
- Audio visual and photographic services. Visual Information Command has supported 2,463 events to date supporting POTUS, VPOTUS, First Lady and senior staff.
- White House Continuity of Government requirements.

Net funding changes from FY 2009 through FY 2010 result from reductions in operational support requirements and realignment of civilian payroll as a part of DISA initiative to enhance the civilian management process and more accurately report civilian payroll costs for each DISA program. Additionally, non-pay funds were realigned to support WHCA's increase of 50 civilian Full Time Equivalents (FTE) starting in FY 2010. The increase in FTEs will assist with the new administration and mission requirements.

b. White House Situation Support Staff (WHSSS) (FY 2010: $6,302 thousand): The White House Situation Support Staff (WHSSS) was created by Presidential direction. The WHSSS provides classified communications, computer, and intelligence systems for the National

I. Description of Operations Financed: (continued)

Security Advisor, White House Situation Room, the NSC staff, and other White House offices. The WHSSS funds support the information systems used by the NSC and others.

The FY 2010 funding will support upgrades to the classified and the unclassified network systems used by the Situation Room and the NSC. Additionally, systems essential to the NSC data replication project were funded which ensures that critical NSC documents are stored for retrieval under a variety of scenarios.

c. Crisis Management System (CMS) (FY 2010: $10,018 thousand): The Crisis Management System (CMS), owned by the NSC, operated and maintained by DISA under NSC direction, provides state-of-the-art video teleconferencing (SVTS), Crisis Management Network (CMN), and the Executive Voice-over Secure IP (VoSIP) phone network (including the National Intelligence Watch Officers Network) to the President, Vice President, National Security Advisor, and others in both fixed and mobile modes for exchange of time sensitive high interest information, extending White House Situation Room presence. Funding covers the cost of maintenance, configuration management, certification and accreditation activities including system security monitoring and testing, and engineering support.

d. Minimum Essential Emergency Communications Network (MEECN) (FY 2010: $5,575 thousand): Minimum Essential Emergency Communications Network (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

I. Description of Operations Financed: (continued)

together provides a management structure that ensures seamless engineering, plans and procedures, and operational assessment support of these capabilities. Funding changes are from realigned payroll costs and congressional adjustments.

e. Communications Management Control Activity (CMCA) (FY 2010: $1,310 thousand): Communications Management and Control Activity (CMCA) funding provides for travel, training, ADP, supplies and a maintenance contract for the CMCA Automated Tracking Tool. All funds provide the DISA liaison mission support to the US Secret Service in support of the protective mission for visiting heads of state, and national special security events. Support is also provided to the Joint Staff, J3/Joint Directorate of Military Support (JDOMS), for communications at national and international sporting events approved by the US Attorney General and Congress. Funding changes are from realigned payroll costs.

II. Force Structure Summary: N/A

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2010 Budget Estimates

III. Financial Summary ($ in thousands)

A. BA 4 Subactivities	FY 2008 Actuals	FY 2009 Budget Request	FY 2009 Congressional Action Amount	FY 2009 Congressional Action Percent	FY 2009 Appropriated	FY 2009 Current Estimate	FY 2010 Estimate
1. Transition to Net Centric Environment	94,753	170,850	-271	-0.16%	170,579	170,579	200,203
2. Eliminate Bandwidth Constraints	256,834	156,915	-84	-0.05%	156,831	156,831	147,765
3. GIG Network Operations and Defense	324,614	443,353	-5,736	-1.29%	437,617	437,617	512,649
4. Exploit the GIG for Improved Decision Making	171,926	233,349	-25,988	-11.14%	207,361	207,361	226,039
5. Deliver Capabilities Effectively/Efficiently	102,164	68,466	1,493	2.18%	69,959	69,959	86,387
6. Special Missions	153,882	154,693	-483	-0.31%	154,210	154,210	149,120
Total BA 4	1,104,173	1,227,626	-31,069	-2.53%	1,196,557	1,196,557	1,322,163

*The FY 2008 Actual column includes $44,510 thousand of Consolidated Appropriations Act, 2008, Division L, Supplemental Appropriations, Defense (PL 110-161), $105,794 thousand of Supplemental Appropriations Act, 2008, Title IX, Defense Matters, Chapter 1, Defense Supplemental Appropriations for Fiscal Year 2008 (PL 110-252), and includes $3,611 thousand of No-Year Spectrum Relocation funds.

**The FY 2009 column excludes $31,100 thousand of Bridge Funding Appropriations for FY 2009 (PL 110-329), $118,705 thousand of FY 2009 Overseas Contingency Operations funding, and also excludes $15,309 thousand of No-Year Spectrum Relocation funds.

***The FY 2010 column excludes the request for $245,117 thousand for the FY 2010 Supplemental funding.

III. Financial Summary ($ in thousands)

B. Reconciliation Summary	Change FY 2009/FY 2009	Change FY 2009/FY 2010
Baseline Funding	**1,227,626**	**1,196,557**
Congressional Adjustments (Distributed)	-28,000	
Congressional Adjustments (Undistributed)		
Adjustments to Meet Congressional Intent		
Congressional Adjustments (General Provisions)	-3,069	
Subtotal Appropriated Amount	**1,196,557**	**1,196,557**
Fact-of-Life Changes (CY to CY Only)		
Subtotal Baseline Funding	**1,196,557**	**1,196,557**
Anticipated Supplemental	31,100	
Reprogrammings		
Price Changes		17,386
Functional Transfers		
Program Changes		108,221
Current Estimate	**1,227,657**	**1,322,163**
Less: Wartime Supplemental	-31,100	
Normalized Current Estimate	**1,196,557**	**1,322,163**

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
FY 2009 President's Budget Request (Amended, if applicable)		1,227,626
1. Congressional Adjustments		-31,069
a. Distributed Adjustments	-28,000	
b. Undistributed Adjustments		
c. Adjustments to meet Congressional Intent		
d. General Provisions - Sec 8101 – Economic Assumptions	-2,504	
e. Congressional Earmarks – Mitigation to Environment Impacts	-565	
FY 2009 Appropriated Amount		**1,196,557**
2. War-Related and Disaster Supplemental Appropriations		31,100
3. Fact of Life Changes		
FY 2009 Baseline Funding		**1,227,657**
4. Reprogrammings (requiring 1415 Actions)		
Revised FY 2009 Estimate		**1,227,657**
5. Less: Item 2, War-Related Supplemental Appropriations		-31,100
FY 2009 Normalized Current Estimate		**1,196,557**
6. Price Change		17,386
7. Functional Transfers		
8. Program Increases		108,220
a. Annualization of New FY 2009 Program		
b. One-Time FY 2010 Increases		
c. Program Growth in FY 2010		
1) Senior Leadership Enterprise: Funding increased for classified work (FY 2009 Base: $0 thousand)	55,924	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
2) NCES: Increases in funding support operational sustainment of innovative engineering initiatives ($8,000) and increases in operational support requirements; increased NCES capabilities through FDDR, migration from 9x5 to 24x7, growth in Collaboration Web Conferences usage (FY 2009 Base: $89,247 thousand)	26,749	
3) CNCI: Classified work (includes $14,517 thousand FY 2010 increase) (FY 2009 Base: $32,493 thousand)	30,715	
4) Field Commands: Agency realignment of personnel costs and increase in other DISA requirements; increased funding to support work in innovative solutions ($900 thousand) (FY 2009 Base: $48,885 thousand)	12,964	
5) JTF-GNO: Realignment of funds to establish independent line for JTF-GNO operational support requirements (FY 2009 Base: $181 thousand)	18,679	
6) Shared Services/PEOs: Increase results from an increase in DISANet support services and maintenance contracts; increase in maintenance requirements as a result of new software and hardware added to the DISANet; DISA's efforts to support Chemical, Biological, Radiological, and Nuclear (CBRN) force protection of DISA facilities and personnel as part of the DOD's Joint Project Manager Guardian (JPMG) Program and, operations of DISA Headquarters Facility at Fort Meade, MD (BRAC); increased funding operational requirements for the PEO-STS (FY 2009 Base: $18,825 thousand)	11,387	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
7) NetOps: Net impact of Agency-wide realignment of personnel costs and changes in operational requirements; support for SATCOM, NetOps, and AFRICOM initiatives ($3,500 thousand) (FY 2009 Base: $17,277 thousand)	3,837	
8) CMCA: Increases in operational support requirements (FY 2009 Base: $904)	396	
9) CMS: Increases in operational support requirements (FY 2009 Base: $9,597)	309	
10) WHSSS: Increase in operation support requirements (FY 2009 Base: $6,023)	210	
11) ACTD: Programmatic realignment of civilian personnel salaries and benefits and increased focus on rapid technology projects ($2,800 thousand) (FY 2009 Base: $5,889 thousand)	5,479	
12) CENTRIXS: Net increase from changes in operational support requirements and to establish a centralized coalition NETOPS ($8,140 thousand), and design and implement a global architecture supporting COCOM coalition information sharing (FY 2009 Base: $39,870 thousand)	3,807	
13) JSSC: Increase in equipment requirements and adjustments to civilian pay (FY 2009 Base: $24,556 thousand)	3,497	
14) DIB: Classified requirements (FY 2009 Base: $1,994 thousand)	2,907	
15) PRMRF: Space/Rent change for the Pentagon Reservation (FY 2009 Base: $14,949 thousand)	1,826	
16) DSO: Adjustments in civilian pay and other operational requirements. (FY 2009 Base: $26,774 thousand)	2,256	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
17) PKI: Realignment of personnel costs (FY 2009 Base: $13,171 thousand)	1,564	
18) CWID: Increase in operational support requirements (FY 2009 Base: $2,194 thousand)	92	
19) Other Programs/Counter Drug: Increased operational requirements and realignment of payroll costs (FY 2009 Base: $13,398 thousand)	2,144	
9. Program Decreases		-76,522
a. Annualization of FY 2009 Program Decreases		
b. One-Time FY 2009 Increases - E-Commerce	-13,910	
c. Program Decreases in FY 2010		
1) Mgmt HQs: Adjustments to civilian pay and operational support requirements (FY 2009 Base: $36,066 thousand)	-2,320	
2) GCCS-J: Decrease in fielding activities associated with GCCS-J v4.2 releases. GCCS_J funding ramped down. (FY 2009 Base: $88,570 thousand)	-22,881	
3) Teleport: Net changes in Agency realignment of pay, reduction in operational support requirements, and increased funding to Teleport ($2,100 thousand) (FY 2009 Base: $17,279 thousand)	-6,930	
4) DISN EA: (FY 2009 Base: $91,576)	-2,527	
5) NMCS: Agency realignment of payroll costs (FY 2009 Base: $6,966 thousand)	-2,551	
6) NECC: (FY 2009 Base: $10,893)	-1,386	
7) STEP: (FY 2009 Base: $1,511)	-118	
8) DISN Subscription: Reductions in operations support requirements (FY 2009 Base: $16,302 thousand)	-2,522	

III. Financial Summary ($ in thousands)

C. Reconciliation of Increases and Decreases	Amount	Totals
9) GIG ES: Realignment of payroll costs and reductions in equipment requirements (FY 2009 Base: $73,249 thousand)	-4,587	
10) DMS: Decrease due to Agency realignment of personnel costs, reduction in travel, and equipment requirements (FY 2009 Base: $16,195 thousand)	-2,049	
11) GCSS: Reduction in equipment requirements and adjustments to civilian pay (FY 2009 Base: $17,843 thousand)	-1,838	
12) WHCA: Reduction in pay, travel, contractor support, and equipment requirements (FY 2009 Base: $129,723 thousand)	-5,335	
13) MEECN: Reduction in travel, pay, contractor support, and equipment requirements (FY 2009 Base: $7,963 thousand)	-2,482	
14) GEMSIS: Decrease from changes in operational support requirements and realignment of O&M, DW, to Proc, DW for GEMSIS Increment 1 hardware fielding requirements ($3,389 thousand)	-909	
15) ISSP/IA: Net decrease resulting from increased support for enhanced Privilege Management capabilities ($3,100 thousand); payroll adjustments, changes in other ISSP requirements, internal realignment of funds within GIG operations and movement of funds to MILCON (FY 2009 Base: $299,860 thousand)	-4,177	
FY 2010 Budget Request		**1,322,163**

IV. Performance Criteria and Evaluation Summary

The DISA's approach to performance-budget integration and measurement is through the balanced scorecard (BSC) methodology to manage, monitor and execute the DISA objectives. The pyramid of outcomes is aligned to the DISA's Surety-Reach-Speed strategy and other top-level goals and objectives. The customer perspective portions of the strategy and measures are supported by financial, internal process, and learning and growth perspective related portions of strategies and measures. Targets designed to promote continuous improvement have been identified for each objective.

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) with an owner and have schedule. Scorecard owners brief the DISA senior leadership periodically on progress in executing the strategy. The reviews are valuable because of the opportunity to discuss the strategy on an ongoing basis. The reviews strengthen individual accountability and alignment with Corporate priorities.

The DISA aligns to the fundamental imperatives of agility in support of joint warfighting capabilities and wider asymmetric challenges, and implementing enterprise-wide changes to organizational structures, processes, and procedures supporting strategic direction.

The DISA uses other external measurement methodologies to track performance. Strategies are developed for rectifying readiness deficiencies, and these strategies are addressed in program/budget planning. This data measures the readiness to execute mission essential tasks under the DoD Readiness Reporting Systems (DRRS). Another external measurement used is the performance and budget information for Capital Asset Plan and the Business Case Summary Exhibit 300s required by the Office of Management and Budget Circular A-11. The DISA is also implementing DoD-Wide Continuous Process Improvement

IV. Performance Criteria and Evaluation Summary

(CPI)/Lean Six Sigma (LSS) Program, which includes making improvements in productivity and performance against mission (availability, reliability, cycle time, investment, and operating costs).

Net-Centric Enterprise Services (NCES)

NCES has developed several key metrics to improving operations and maintenance functions by emphasizing quality of services, customer and performance satisfaction, and reduction in overall sustainment costs. Listed below are four (4) key performance metrics, definitions, and the measures to assess Operations and Maintenance performance.

Performance Metric	Description	Measure
Customer Perspective	Proactively answer customer's questions and provide timely solutions to support and enhance job performance.	A favorable rating of 3 out of a possible 4 on the customer satisfaction level as indicated in customer satisfaction surveys
Contractor Performance	Measures how effectively NCES managed service providers are meeting Service Level Agreements (SLAs).	Validated monthly analysis of performance reporting by the managed service providers and independent Enterprise Service Management (ESM).

IV. Performance Criteria and Evaluation Summary

Performance Metric	Description	Measure
Internal Process Perspective	Measures the effectiveness of the PMO in performing program control, executing functions, and meets mission objectives timely and efficiently. NCES will use an Integrated Master Schedule (IMS) as the indicator of program efficiency.	The IMS will be maintained as an interactive project management tool. Action Officers will self report on tasks. Data Includes: Planned Start/End Dates, Actual Start/End Dates, Level of Effort (Planned, Current, Spent), and Progress (percent Complete).
Requirements Satisfaction	Demonstrate that NCES meets or exceeds program requirements as defined in the NCES Capabilities Development Document.	Monthly analysis of collected performance data on core enterprise services and overall system performance.

NCES published the Capability Production Document (CPD) in March 2008, to capture the affordable and supportable capabilities to be delivered during the Production and Deployment Phase. The CPD provides detailed operational performance attributes developed by the operational community, including Key Performance Parameters (KPPs), which provide meaningful performance and workload data for the major milestones.

GIG Engineering Services (GIG ES)

Performance criteria and evaluation of the Systems Engineering Center (SEC) mission can be divided into two areas: 1) systems engineering, modeling and simulation and 2) interoperability standards. The SEC's systems engineering, modeling and simulation

IV. Performance Criteria and Evaluation Summary

area is measured by its impact on DoD communications planning and investment strategy, with criteria based on SEC's performance of a broad spectrum of technical activities. These include application assessments, contingency planning, network capacity planning and diagnostics, system architecture evaluation, technical and operational assessments of emerging technologies, and systems-level modeling and simulation.

Specific Measures of Success (MOS) and Performance Criteria (PC) for the IT Standards mission are as follows:

Standards Engineering:
(MOS) Achieve full implementation of the GIG Technical Documentation (GTD) repository and witness DOD wide community acceptance and use.
(PC) GTD content updated on schedule to maintain relevance and DECC hosting of web enabled repository maintains 95 percent or greater application availability.
(MOS)GTD is federated along with the DOD IT Standards Registry (DISR) in support of the ASD/Joint Staff J6 system certification process.
(PC)Customer satisfaction for accessing, declaring content and measuring compliance will be assessed/surveyed.

Standards Management:
(MOS)Interoperability Enhancement Process (IEP) for Tactical Data Link family completes pilot phase and migration of all TDL system implementation data resident in the iSmart database.
(PC) iSmart web enabled content updated on schedule to maintain relevance and DECC hosting maintains 95 percent or greater application availability.
(MOS)IEP process achieves automated configuration management capability for the family of TDL standards.

IV. Performance Criteria and Evaluation Summary

(PC)Measured reduction in costs associated with the elimination of manual processes and ability to measure immediate cost impacts to system implementations as TDL standards evolve/change.

Net Ready Technical Assessment:
(MOS)Assessment processes achieves automated/virtual review of technical compliance under federated repositories vice review of JCIDS (text) documents.
(PC) Measured reduction in costs associated with the processing and analysis of JCIDS capabilities documentation.
(MOS)JCPAT "audit" module completed and applied against Net Ready KPP content declared by PMs.
(PC)Audit module improves accuracy and speed (turnaround) of reviews back to PM and measures aggregate level of use/compliance with Enterprise Wide Service Profiles (EWSE) and other systems engineering guidance contained in the GTD.

The Chief Technology Officer's (CTO) task order is composed of multiple short-suspense technology research/exploration components with a concrete deliverable targeted at a facet of the mission. Each research initiative is produced in collaboration with a designated task subject matter specialist. These engineering tasks are short term in nature and designed to facilitate high-potential over-the-horizon technology into engineering programs supporting the mission. Engineering support is provided for CTO technical reviews of DISA programs, at least 4 reviews supported per month.

IV. Performance Criteria and Evaluation Summary

Advanced Information Technology Services-Joint Program Office (AITS-JPO)

Metrics are tracked for each type of technology project within the ITTP, which utilizes JCTDs, Joint Ventures, and Risk Mitigation Pilots to support DISA's 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. Senior level collaborations develop each JCTD proposal based on integrated priority lists. The JCTDs focus on resolving the joint, combined, coalition, and interagency warfighting and operational problems of the COCOMs within a one-to three-year timeline. The JCTDs address problems primarily by conducting technology and operational demonstrations and operational utility assessments (OUA) of mature technology/solutions (TRL 5-7) and transitions to the acquisition community for post-JCTD development, production, fielding, and operation and maintenance (O&M).

The JCTDs fill the gap between science and technology (S&T) and acquisition for the COCOM customer through strong partnerships with the military services and agencies. The JCTDs are not acquisition programs or science projects. Senior leadership within the OSD, R&D, and JCTD community reviews the proposal and subjects it to additional requirements scrutiny by the Joint Requirements Oversight Council to eliminate any duplication of effort. Proposals approved by senior leadership become formal JCTDs.

The next step for the JCTD is to develop an Implementation Directive and a Management Plan. These guidance documents involve a general/flag officer commitment between OSD, DISA, and the COCOM. The basic objectives, schedule, and funding for the JCTD are then outlined. During the first year, the JCTD develops and documents the detailed objectives against which the Operational Sponsor (a Combatant Command) will assess military utility, and outline detailed mechanisms by which military utility will be assessed and measured. Each JCTD project develops a schedule and detailed objectives, usually using a spiral

IV. Performance Criteria and Evaluation Summary

methodology, with incremental demonstrations, limited utility assessments of the demonstrated capabilities, and refinement of future capabilities based on feedback.

The COCOMs use the Military Utility Assessment as a tool to evaluate JCTD products. Status is maintained on the progression of each JCTD in accordance with scheduled developed and published in the Management Plan and funding identified in the Implementation Directive. Regular oversight is maintained through JCTD program managers who are the central point of contact for maintaining cognizance over cost, schedule, and performance and for managing program risk. The ITTP incorporates internal processes to enhance financial reporting and track contractor spending. Monthly reports provide timely information on contractor expenditures. The ITTP utilizes several web-based financial management tools to obtain budget and execution information. The JCTDs are a focused effort to transition technical and operational products (i.e., capability hardware, software, documentation) into an enduring operational capability, using a "try with the intent to buy" approach. The ITTP evaluates additional internal measures, including timeliness of equipment purchases, travel, and demonstration support to assess if each requirement effectively meets mission requirements.

To accomplish the innovation technology transformation projects, DISA is pursuing partnering with FFRDCs and other S/A/C research laboratories, using open source solutions, and developing a DISA Enterprise Management sustainment approach. The DISA will leverage all existing and relevant existing investments in RACE, Capacity on Demand, and FORGE.mil, since these capabilities take advantage of standards-based platforms and reduce development, deployment, and sustainment costs. The DISA will establish a Technology Investment Board able to assess proposed technologies and make quick investment decisions for technology exploration. The DISA's steps to innovation will include identifying high

IV. Performance Criteria and Evaluation Summary

pay-off targets, analysis by the Technical Assessment Center, early horizontal and vertical integration, and transition into Programs of Record.

Coalition Warrior Interoperability Demonstration (CWID)

Annual assessments of the technologies are completed by the Joint Interoperability Test Command (JITC), and a comprehensive Annual Performance Report is produced using these assessments and other input by the CWID staff. This document is reviewed by the Senior Management Group and host COCOM. The CWID Performance Report determines effectiveness of CWID program to facilitate fielding and advancement of C4 net-centric capabilities.

DoD Teleport Program

Teleport manages and tracks its cost and schedule performance parameters using a tailored Earned Value Management System (EVMS) process, integrating the program plan, the program schedule, Work Breakdown Structure (WBS), and financial data. Progress is monitored and documented monthly showing percentages complete of schedule and cost. Formal updates with changes to the schedule are documented against the program baseline. The PEO-STS performance metrics will include: 1) Integrated Master Plan Reviews; 2) Director's In-Progress Review (IPR); 3) PEO-STS Status of Funds (SOF); 4) System Engineering Plan Reviews (SEP); 5) SE Process Assessment Reviews; 6) Property Accountability; 7) Occupation Evaluation Plan (OEP)/ SAFETY; 8) Reconciliation of the Government Purchase Card; 9) PCM Project Over Arching Work Group (OAWG); 10) Acquisition Strategy Approval Decision; 11) Weekly Plans, Program & Control (PPC) session; 12) JIPM Risk, Schedule, Planning Session (RSP); and 13) Acquisition of Services Data Collection Requirements.

The PEO program level Integrated Master Schedule (IMS) defines the milestones and decision and integration points for the program management offices. The IMS provides insight into the critical paths of the program offices. Each review is an intermediate

IV. Performance Criteria and Evaluation Summary

milestone for the determination of progress achieved for each performance metric. The funding covers contractor support needed to establishing, developing, monitoring, and reporting of performance metrics.

Standardized Tactical Entry Point

STEP manages and tracks its cost, schedule, and performance parameters based on the STEP Program Plan, the program schedule, and financial data. Schedule, performance, and customer satisfaction measures are compiled both as a real-time barometer on present customer's satisfaction and predicting success of quality and reliability in future STEP goals and objectives. Progress is monitored and documented monthly, with formal updates occurring during the Wideband quarterly schedule meetings.

Specific Performance Metrics:	FY 2008	FY 2009 & FY 2010
Number of DISN TE Sites	-	3 Planned
Number of Missions	2400 Target Met	2000 Planned
Reliability	99.9 percent Target Met	99.9 percent Planned
Availability	99.9 percent Target Met	99.9 percent Planned

Global Electromagnetic Spectrum Information System (GEMSIS)

GEMSIS performance will be managed and tracked using a tailored Earned Value Management (EVM)-like process. This process integrates the program plan, program schedule and work breakdown structure, and financial data to determine program efficiencies. Progress is monitored and documented monthly showing percentages complete of schedule and cost that will be used as a decision-making tool for the Program manager, ensuring timely delivery of the capability to the customer. Formal updates with changes to the schedule are documented against the program baseline.

IV. Performance Criteria and Evaluation Summary

Defense Information Systems Network (DISN)

The primary performance metrics are:	FY 2008	FY 2009 & FY 2010
Number of ATI circuits transitioned per week. 15 actual (2008)	30 Target Not Met	35 Planned*
Quarterly Product Support Reviews for Tech Refresh	-	1 per quarter
Fully reimburse the DWCF for Kosovo costs within 98 percent of planned cost	Target Met	Planned
Ensure network availability of DSCS ≥ 99.99 percent	Target Met	Planned
Ensure switch systems can support survivable nuclear command and control mission for EPC/SECN ≥ 99.99 percent	Target Met	Planned
Fully reimburse the DWCF for Supplemental costs within 98 percent of planned cost	-	Planned

* A Tiger Team was established to improve the number of circuits transitioned which is on schedule to meet metric.

IV. Performance Criteria and Evaluation Summary

The SATCOM/Wireless Engineering Division and the GIG Network Engineering Division/RF Networking Section conduct regularly scheduled In-progress Program Reviews (IPRs) meetings to monitor status of engineering projects/tasks. Each current project/task is evaluated in the progress of the technical work and how efficiently allocated resources are being utilized. As a result, adjustments are made to resources, schedules, and technical directions. Future projects/tasks are also discussed, to ensure an integrated approach is maintained across related project/task areas.

Satellite Communications (SATCOM) Program Management Office (PMO) manages and tracks its cost and schedule performance parameters using a tailored Earned Value Management (EVM) system and process, integrating the program plan, the program schedule, Work Breakdown Structure (WBS), and reconciling the financial data. Progress is monitored regularly and updates and changes are documented against the WBS and EVM.

Network Operations and Defense (NetOps)

The NetOps performance measures include:

- Percentage of detected intrusions to the networks; time to detect intrusions; downtime due to intrusions; and percentage of sensors detecting/reporting intrusions
- Number of countermeasures produced to deter threats to the networks; amount of time required to develop countermeasures
- Number of CNDSP providers accredited with environmental reviews conducted

Information Systems Security Program (ISSP)/ IA PKI (PKI)

The DISA is implementing the GIG Information Assurance Program (GIAP) comprehensive capability-based management system, integrating strategic planning objectives with day-to-day operational/programmatic/technical management processes, using a cascading system of linked performance measures that includes:

IV. Performance Criteria and Evaluation Summary

- Maintain directory of DoD personnel identification information
- Establish & maintain IA network policy
- Assess vulnerabilities
- Validate policy compliance
- Develop & implement secure architecture
- Develop & implement secure network components
- Detect unauthorized access or misuse
- Identify vulnerabilities
- Establish standard configurations
- Provide situational awareness
- Detect attacks across the GIG
- Correlate incidents for analysis
- Harden internal DoD Networks
- Attribute and respond to improve real time response actions

The PKI system allows users and information assets to be authenticated in DoD networks and applications. This infrastructure includes individual and device certificate users in the PKI system to access DoD networks and applications securely while maintaining data and system integrity. Performance indicators are:

- Enabled GIG to provide identity based services to DOD system
- Protect applications from unauthorized access
- Protect boundary from unauthorized access
- Detect unauthorized access or misuse
- Detect unauthorized access by intruders & malicious codes

IV. Performance Criteria and Evaluation Summary

- Defense Critical Infrastructure Protection
- Ensures effective, efficient, and secure information flow

Field Commands and Field Offices

Each Field Command/Field Office serves as the customer's advocate to DISA and assists customers by providing technical assistance and management support in planning, systems engineering, and implementation of DISA's core products and services. A bi-annual performance assessment is performed by the Joint Staff J8 Combat Support Agency Review Team (CSART), customer surveys, semi-annual COCOM J6 conferences and annual DISA Partnership Executive Forum chaired by the DISA Director.

To measure performance and budget integration, the Field Commands and Offices track and submit a quarterly Balanced Scorecard (BS). The BS allows reporting of accomplishments relating to the DISA missions, down to specific topics.

Metrics currently being used include:

- Defense Readiness Reporting System Measures.
- Fiscal stewardship - Manage all costs, including external and internal costs, to ensure best value for the customer.
- Balance Scorecard measures for Transform DISA NetOps Centers - Deliver improved required capabilities more effectively, economically, and efficiently.
- Warfighter/COCOM support - Provide theater-wide secure, robust, interoperable communications, networks and customer support to COCOMS, Service components, NATO, coalitions and U.S. government agencies.
- First Line Support to COCOMs - Improve the process of fielding new technology by exchanging ideas, clarifying roles and responsibilities, and understanding impacts.

IV. Performance Criteria and Evaluation Summary

- Letter input from COCOM J6s for DISA Commanders' performance appraisals.
- Combat Support Agency Review Team survey of all COCOMs and Services rated by using the DISA Mission Essential Task List standards.

Joint Staff Support Center (JSSC)

The JSSC tracks performance and results through system and problem ticket metrics, Internal Performance Reviews (IPRs), Balance Scorecard results and customer surveys. If performance standards are not being met by the GIG a thorough and complete evaluation/audit of the underperforming area will be performed to determine the barriers to performance, source and contributors to poor performance and ultimately corrective action that must be taken to get an initiative back on track.

Joint Task Force-Global Network Operations (JTF-GNO)

The JTF-GNO performance measures include:

- Number of resolved/assisted issues in 63,000 communications/network worldwide-generated, 500 directives and warning orders
- Number of formal reviews of 5,000 software vulnerabilities, issued 50 alerts, 30 bulletins, and 50 technical advisories to eliminate/mitigate vulnerabilities
- Achieving decreases in the number of successful intrusions of the GIG by improving perimeter security, and focusing on protecting web servers
- Identifying and decreasing the number of "remotely controlled" DoD computers
- Response time of crisis action team following major undersea cable cuts
- Identification of major exploitations and compromises in networks and orchestrate reporting, remediation, and resolution issues prior to GIG-wide spread

IV. Performance Criteria and Evaluation Summary

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

Cost & Schedule Management – GCCS-J and CFAST utilize earned value management to manage technical cost and schedule requirements. Contractors are required to plan, budget, and schedule resources in time-phased "planned value" increments constituting a cost and schedule measurement baseline. This approach encourages contractors to use effective internal cost and schedule management control systems. Performance is evaluated by conducting contractor performance reviews and weekly critical path reviews of the CFAST release schedules to track tasks and mitigate risk through the entire lifecycle.

Global Combat Support System (GCSS) Combatant Command/Joint Task Force (CC/JTF)

In FY 2010, GCSS (CC/JTF) is fielding critical capabilities that implement JS validated, approved, and prioritized functional requirements contained in the approved GCSS Capabilities Development Document (CDD). The CDD is translated into technical solutions with approved cost, schedule, and performance parameters. In addition, GCSS (CC/JTF) intends to undertake development, integration, testing, and fielding of capabilities within an approved capability increment plan. The capabilities include decision support tools; the integration of additional data sources and federated applications; and the implementation of a new Enterprise Information Integration (EII) tool and Business Intelligence tools that support the Department's Net-Centric Vision often exposing and consuming data and applications as web services.

National Military Command System (NMCS)

The NMCS Engineering Branch conducts regularly scheduled In-progress Program Reviews (IPRs) and Configuration Control Board (CCB) meetings to monitor status of engineering projects/tasks. Each current project/task is evaluated in terms of progress on the technical work and how allocated resources are being utilized. Adjustments to resources,

IV. Performance Criteria and Evaluation Summary

schedules, and technical directions are made, as required. Future projects/tasks are discussed to ensure an integrated approach is maintained across related project/task areas. The utility of the IPR/CCB structure is increased because the Joint Staff customer participates in the project/task reviews. The result of this approach is an integrated common goal achievement with NMCS Engineering, contractor, and Joint Staff.

Defense Message System (DMS)

Key Joint Staff - validated performance metrics:

	FY 2008	FY 2009 & FY 2010
Availability of DMS Backbone & Local Sites:	≥ 99 percent Target Met	≥ 99 percent Planned
Directory Search Results to User:	≤ 5 sec Target Met	≤ 5 sec Planned
Message Delivery (sender to recipient)	≤ 3 min Target Met	≤ 3 min Planned

Combined Enterprise Regional Information Exchange System (CENTRIXS)

The Multinational Information Sharing (MNIS) Program Office for CENTRIXS uses an internal process to provide monthly expenditure financial reports and tracking of contractor spending. Other internal measures such as timeliness of equipment buys and travel are reviewed and evaluated for cost control and assurance to meet requirements.

Centralization of CENTRIXS services yields qualitative performance measures by increasing the availability and security of Coalition Information Sharing over the previous decentralized approaches unique to the various COCOMs. Execution of CCER will enable reductions in "touch labor" yielding over $32M in savings.

IV. Performance Criteria and Evaluation Summary

Griffin performance criteria are based on the introduction of new information sharing services as driven by the CCEB direction. Successful achievements include introduction of US/UK Common Operational Picture and successful testing of Cross Domain Collaborative Information Environment (CDCIE) cross domain chat on CFBLNet.

CFBLNet performance criteria are measured by the number of successful trials (measured in the hundreds) supported throughout the year on the CFBLNet infrastructure with special focus on the complex support provided annually to the Coalition Warrior Interoperability Demonstration (C2 focus) and the Empire Challenge (ISR focus) exercise.

Net-Enabled Command Capability (NECC)

The NECC recently updated the cost control plan in conjunction with the Cost Analysis Improvement Group (CAIG), OUSD (AT&L), and OUSD (PA&E) that describes both earned value (EV) management and performance metrics.

The cost control plan implemented an EV pilot to provide EV information for monitoring the program's cost, schedule, and technical performance. NECC's EV pilot has two main areas, the NECC Joint Program processes and CM development. The NECC internal support costs are consolidated monthly and tracked against a Planned Value baseline and EV milestones. The EV for the CM development approach includes establishing a Planned Value baselines and milestones for each CM. Monthly reports define the actual costs incurred and milestone dates. In summary, the EV for both the Joint Program and CM development is realized when a milestone is considered to be 100 percent complete.

The Program Office is collecting and analyzing a broad set of performance metrics to evaluate performance of the end-to-end NECC process. Essential criteria for validating the NECC business strategy is gathered through performance measurement data collected

IV. Performance Criteria and Evaluation Summary

over the course of the program. The aggregated data obtained from NECC end-to-end process surveillance and CM development metrics are used to define a baseline of repeatable performance for all stages of the acquisition process.

Minimum Essential Emergency Communications Network (MEECN)

Performance of the Nuclear C3 System is measured by the operational assessments funded in this program element. These periodic assessments evaluate the connectivity used for the five functions of NC2: Situation Monitoring, Planning, Decision Making, Force Execution, and Force Management. Assessment results are used by the Joint Staff to direct changes in system engineering and integration, programmatic execution, and training.

Component Execution Executive (CAE):

CAE evaluates its success by monitoring and measuring the following:

- Percent of DISA Major Acquisition Programs delivering within Program Cost, Schedule and Performance baseline through the MAIS Annual Report (MARS).
- Number of major acquisition policy/processes developed and updated. This includes the development, issuance, and educational outreach for acquisition policy instructions, guidelines, and reporting templates.
- Percent of DISA staff in acquisition designated positions meeting the Defense Acquisition Workforce Improvement Act (DAWIA) certifications.
- Number of program reviews/decision forums sponsored at the CAE and/or above level. Anticipating an increase in spiraling new capabilities which will increase the number of reviews. Anticipate performance levels will increase due to efficiencies gained through improved processes and increased knowledgeable and experienced workforce.

IV. Performance Criteria and Evaluation Summary

Office of Chief Information Officer and Strategic Planning Directorate (CIO)

The DISANet performance is measured by automated systems that compute system availability and responsiveness. Availability represents the percentage of time that networks, servers, and critical applications and systems are available for use. Calculations are based on averages of availability over a 12- month period, on a 24/7 basis, for DISANet sites worldwide. Measurements include scheduled and unscheduled outages. The DISANet E-Mail response time is the average amount of time for a message to be sent and received to DISANet locations as specified, as measured from DISA HQS. The DISANet critical server/application availability refers to the average percentage of time that DISANet services and critical applications are available for use.

	Current Results	Target
DISANet WAN Availability	99.7 %	99 %
DISANet Critical Server/Application Availability	99.4 %	99 %
DISANet NCR E-Mail Availability	99.8 %	99 %
DISANet Non-NCR E-Mail Availability	98.1 %	95 %
NCR E-mail Response Time	105 Sec	300 Sec
Non-NCR E-mail Response Time	221 Sec	600 Sec

DISA Intranet Services and DKO: The DISA Intranet Services and DKO provide a single point of access to enterprise information by providing an underlying infrastructure and set of processes that facilitate the integration of information and knowledge.

Migration from the current EDGE portal to the new DoD enterprise DKO portal infrastructure is a Director-level initiative. To assess the accomplishment of this migration initiative, the following measures were established:

IV. Performance Criteria and Evaluation Summary

- Percentage of DISA personnel (civilian, military, contractors) with DKO accounts
- Ratio of Unique Visits to the number of Active DISA DKO Account holders (per month)
- Percentage of DISA web applications integrated with the DKO SSO infrastructure
- Combined number of DISA DKO organization sites and DISA sponsored Joint Sites

Management Headquarters (MP/PA)

1 Supports the President's Management Agenda Initiative No. 1 – Strategic Management of Human Capital

2 Supports the following Balanced Scorecard Goals:
LG1 – Average number of days to fill vacancies
LG1 – Percentage of Employees Satisfied at DISA (Satisfaction Survey)
LG1 – Percentage of DISA Employees participating in the DISA Telework Program
LG1 – Attrition Percent of total DISA Workforce
LG2 – Percentage of Eligible Employees participating in the Career Management Programs

Comptroller Financial Executive (CFE)

The Balanced Scorecard metrics are collected to measure progress against goals in response to the President's Management Agenda of Improved Financial Performance. Measurements include:

- accomplishing milestones to achieve a clean audit opinion
- meeting budget execution (obligation/disbursement) targets
- supporting Business Transformation Agency in achieving milestones for DISA's implementation of DAI
- scoring of a four or higher by OMB on all IT300 budget exhibits
- decreasing aged payables and receivables

IV. Performance Criteria and Evaluation Summary

- improving or sustaining DoD IG scores on agency financial statements
- maintain reconciliations of cash, accounts payable, and accounts receivable

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2010 Budget Estimates

V. Personnel Summary	FY 2008	FY 2009	FY 2010	Change FY 2008/ FY 2009	Change FY 2009/ FY 2010
Active Military End Strength (E/S)	**1,473**	**1,654**	**1,651**	**+181**	**-3**
Officer	342	420	417	+78	-3
Enlisted	1,131	1,234	1,234	+103	0
Reserve Drill Strength (E/S)	**62**	**103**	**103**	**+41**	**0**
Officer	39	61	61	+22	0
Enlisted	23	42	42	+19	0
Civilian End Strength	**2,433**	**2,413**	**2,712**	**-20**	**+299**
U.S. Direct Hire	2328	2308	2599	-20	+291
Total Direct Hire	2328	2308	2599	-20	+291
Foreign National Indirect Hire	5	5	5	0	0
Memo: Reimbursable Civilians Included	100	100	108	0	+8
Active Military Avg Strength	**1,564**	**1,654**	**1,651**	**+90**	**-3**
Officer	381	420	417	+39	-3
Enlisted	1,183	1,234	1,234	+51	0
Reserve Drill Avg Strength (A/S)	**68**	**83**	**103**	**+15**	**+20**
Officer	42	50	61	+8	+11
Enlisted	26	33	42	+7	+9
Civilian FTEs	**2,440**	**2,382**	**2,679**	**-58**	**+297**
U.S. Direct Hire	2,354	2,292	2,581	-62	+289
Total Direct Hire	2,354	2,292	2,581	-62	+289
Foreign National Indirect Hire	5	5	5	0	0
Memo: Reimbursable Civilians Incl	81	85	93	+4	+8
Average Annual Civilian Salary ($)	**94,977**	**98,681**	**103,560**	**+3,704**	**+4,879**

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2010 Budget Estimates

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

OP 32 Line	FY 2008 Actuals	Change FY 2008/FY 2009 Price	Change FY 2008/FY 2009 Program	FY 2009 Estimate	Change FY 2009/FY 2010 Price	Change FY 2009/FY 2010 Program	FY 2010 Estimate
101 Exec, Gen'l & Special Schedules	223,576	8,486	-5,885	226,177	5,610	35,501	267,288
103 Wage Board	62,083	2,356	-1,286	63,153	1,566	9,269	73,988
107 Voluntary Sep Incentives	413	0	-413	0	0	0	0
111 Disability Compensation	833	0	80	913	0	-13	900
199 Total Civ Compensation	**286,905**	**10,842**	**-7,504**	**290,243**	**7,176**	**44,757**	**342,176**
308 Travel of Persons	31,039	404	-3,895	27,548	331	14,444	42,323
399 Total Travel	**31,039**	**404**	**-3,895**	**27,548**	**331**	**14,444**	**42,323**
672 Pentagon Reserv Maint	11,798	1,629	1,522	14,949	-608	1,625	15,966
673 Def Fin & Accntg Svc	7,141	-371	13	6,783	-14	-3,040	3,729
677 Comm Svcs Tier 1	23,972	-1,247	-7,203	15,522	124	-2,155	13,491
699 Total Purchases	**42,911**	**11**	**-5,668**	**37,254**	**-498**	**-3,570**	**33,186**
771 Commercial Transport	1,669	22	1,466	3,157	38	-62	3,133
799 Total Transportation	**1,669**	**22**	**1,466**	**3,157**	**38**	**-62**	**3,133**
912 GSA Leases	2,288	57	19,248	21,593	540	-5,003	17,130
913 Purch Util (non fund)	3,890	51	-288	3,653	44	693	4,390
914 Purch Communications	40,146	522	-15,435	25,233	303	-470	25,066
915 Rents, Leases (non GSA)	255	3	-142	116	1	48	165
917 Postal Svc (USPS)	97	0	121	218	0	3	221
920 Supplies/Matl (non fund)	15,510	202	-7,525	8,187	98	-60	8,225
921 Print & Reproduction	288	4	3	295	4	6	305
922 Eqt Maint Contract	511,007	6,643	82,768	600,418	7,205	95,427	703,050
923 Facilities Maint Contr	12,199	159	-1,002	11,356	136	960	12,452
925 Eqt Purch (non fund)	45,694	594	3,036	49,324	592	-10,068	39,848
931 Contract Consultants	1,304	17	-6	1,315	16	-541	790
932 Mgt Prof Support Svcs	668	9	-424	253	3	-181	75
933 Studies, Analysis & Eval	37	0	268	305	4	-197	112
934 Engineering & Tech Svcs	5,156	67	-300	4,923	59	-2,456	2,526
987 Other IntraGovt Purch	37,734	491	5,160	43,385	521	-14,319	29,587

Defense Information Systems Agency
Operation and Maintenance, Defense-Wide
Fiscal Year (FY) 2010 Budget Estimates

OP 32 Line	FY 2008 Actuals	Change FY 2008/FY 2009 Price	Change FY 2008/FY 2009 Program	FY 2009 Estimate	Change FY 2009/FY 2010 Price	Change FY 2009/FY 2010 Program	FY 2010 Estimate
988 Grants	150	2	-112	40	0	0	40
989 Other Contracts	65,039	846	1,811	67,696	812	-11,508	57,000
998 Other Costs	187	2	-144	45	1	317	363
999 Total Other Purchases	**741,649**	**9,669**	**87,037**	**838,355**	**10,339**	**52,651**	**901,345**
9999 TOTAL	**1,104,173**	**20,948**	**71,436**	**1,196,557**	**17,386**	**108,220**	**1,322,163**

*The FY 2008 Actual column includes $44,510 thousand of Consolidated Appropriations Act, 2008, Division L, Supplemental Appropriations, Defense (PL 110-161), $105,794 thousand of Supplemental Appropriations Act, 2008, Title IX, Defense Matters, Chapter 1, Defense Supplemental Appropriations for Fiscal Year 2008 (PL 110-252), and includes $3,611 thousand of No-Year Spectrum Relocation funds.

**The FY 2009 column excludes $31,100 thousand of Bridge Funding Appropriations for FY 2009 (PL 110-329), $118,705 of FY 2009 Overseas Contingency Operations funding, and also excludes $15,309 thousand of No-Year Spectrum Relocation funds.

***The FY 2010 column excludes the request for $245,117 thousand of Overseas Contingency Operations funding.

(This page intentionally left blank.)