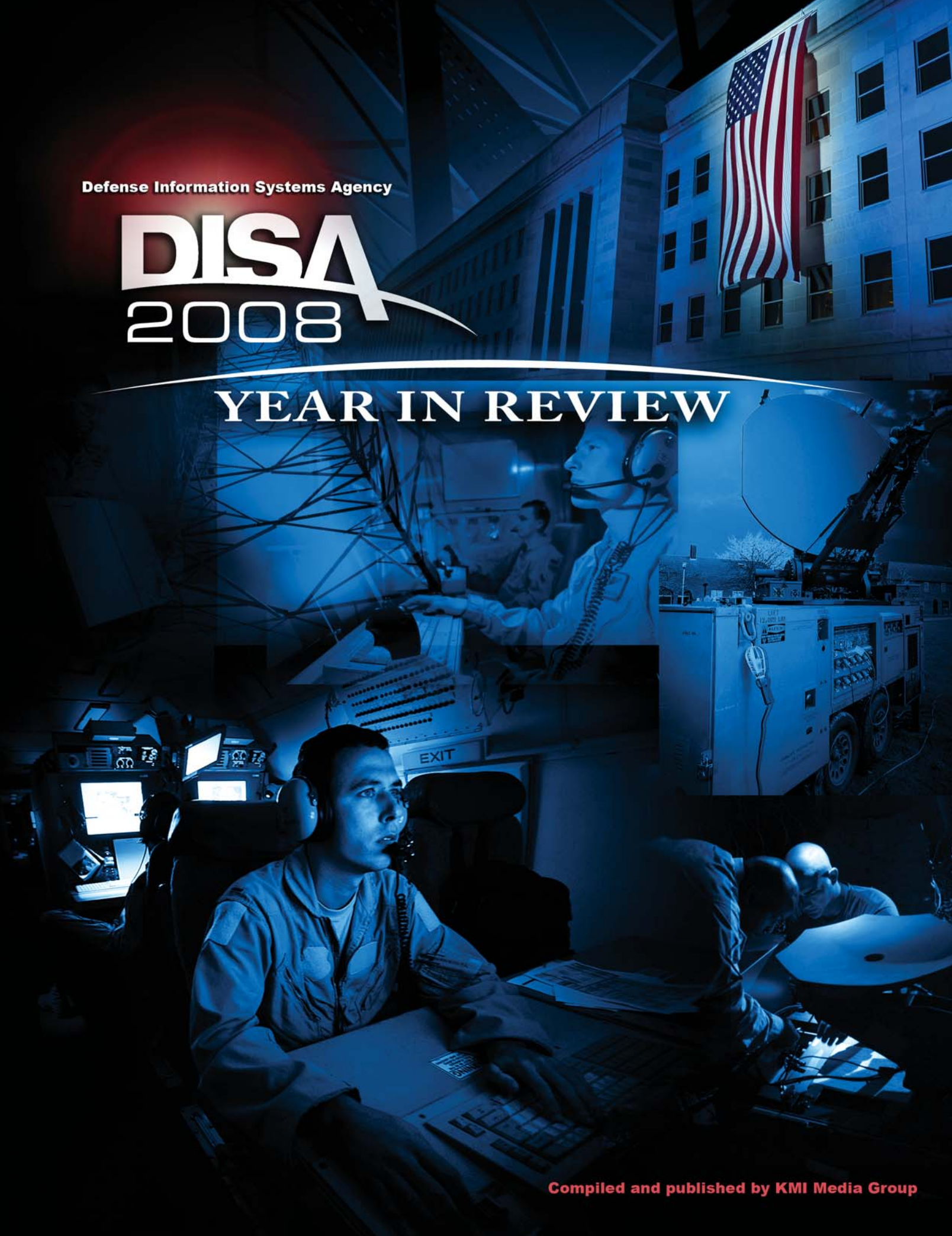


Defense Information Systems Agency

DISA 2008

YEAR IN REVIEW



Compiled and published by KMI Media Group

THE SAFETY OF THE NATION RELIES ON YOUR SYSTEM. WHAT DOES YOUR SYSTEM RELY ON?

Whether you need proactive mission-critical support or basic system maintenance, SSTEW is the answer. Sun Support Total Enterprise Warranty (SSTEW) helps keep your critical Sun™ systems up and running perfectly. Always. It reduces your enterprise's back-end costs with volume discounts, contract management and some of the industry's most sophisticated asset tracking tools. So get SSTEW, the ultimate purchasing vehicle for all of your Sun Microsystems support and warranty services. Because a lot is relying on your IT.



Call 877-SSTEW-96 or visit SSTEW.com to learn what SSTEW can do for you.



Publisher's NOTE

KMI Media Group, publisher of *Military Information Technology*, produced the 2008 DISA Year in Review. The magazine, which publishes 11 times each year, reports on a wide range of C4ISR issues.

The Rockville, Md., company also publishes *Military Geospatial Technology*, *Military Logistics Forum*, *Military Medical Technology*, *Military Advanced Education*, *Military Space & Missile Forum*, *Military Training Technology* and *Special Operations Technology*.

This report was designed by the KMI Media Group Art Department.

Copyright 2009.

KMI Media Group
15800 Crabbs Branch Way
Suite 300
Rockville, Md. 20855
Telephone: (301) 670-5700
Fax: (301) 670-5701
www.mit-kmi.com

DISA did not endorse this report or the advertisements it contains.

For nearly 50 years, DISA has served countless warfighters by providing reliable, innovative communications and information technology solutions. Because it is impossible to detail DISA's many achievements during 2008 in a short compendium, this publication focuses on the progress of some of DISA's major programs and initiatives in the past year.

CONTENTS:

DISA's Support of Operations Iraqi Freedom and Enduring Freedom	2
DISA's Network Services	5
Global Information Grid Enterprise Engineering	8
Net-Centric Enterprise Services	12
RACE and Cloud Computing	14
GIG 2.0: The Next Big Wave	16
The Challenges of Information Assurance	17
BRAC Relocation of DISA Headquarters to Fort Meade	19

DISA'S SUPPORT OF OPERATIONS IRAQI FREEDOM AND ENDURING FREEDOM

DISA is well known by the information communications technology (ICT) community for its strategic global communications mission, especially as the provider of the Department of Defense's global information grid (GIG) backbone. There is, perhaps, less awareness of the agency's role as a partner with all the services and other agencies in supporting the combatant commands' deployed forces with agile, adaptive and capabilities-based information services.

The premier example of DISA's end-to-end, "all the way to the foxhole" support is its critical information-enabling role in Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) in Afghanistan. These operations have demanded the greatest degree of information and communications infrastructure growth in the shortest time period in the history of warfare. Let's look at DISA's initial, ongoing and likely future contributions to the warfighters in this critical theater of operations for a context to understand the DISA role.

INITIAL COALITION WAR FIGHTING SUPPORT

Shortly after September 11, 2001, it became evident that the existing barebones GIG ICT infrastructure in the Central Command (CENTCOM) region would need to be dramatically improved to support any medium- or large-scale operations in the region. Compounding the potentially huge command and control (C2) capability needs were the extreme environmental challenges of deploying new high-technology systems in the most desolate and hostile locations of the Middle East and South Asia.

Existing DoD communications were very limited in bandwidth and used unreliable, single-threaded circuits. They were basically voice and e-mail to a few Persian Gulf stations and mostly "push to talk" to military satellite communications (MILSATCOM) elsewhere. DoD had virtually no communications infrastructure in Afghanistan, Pakistan, Iraq, Qatar and Kuwait.

In preparation for any OEF contingency, DISA recognized the need to reserve commercial satel-

lite communications capacity over the region. Within three weeks following September 11, the first commercial transponder was leased to support flights of Global Hawk, an unmanned aerial vehicle (UAV). Over the next four months, DISA surged the commercial bandwidth capacity for CENTCOM support to more than half a gigabyte. "First rights of refusal" were also purchased as a hedge against the risk of the remaining commercial satellite bandwidth being snatched up by the international media and entrepreneurs.

Simultaneously, DISA successfully defended against mounting pressures to sunset the sustainment of INMARSAT's (an international telecommunications company) on-the-move secure communications capability, anticipating its critical role in Southwest Asian-type environments. Both actions would prove to be key for DISA's readiness to support responsively any yet-to-be-named task forces in the region.

Besides these "leaning forward" actions by DISA, the agency also began acquiring enhanced data, video, imagery and collaboration "information" capabilities in spiral developments to upgrade the capabilities of combat forces as quickly as possible. Some key examples of these accelerated DISA information services were:

- Global Command and Control System-Joint (GCCS-J), which morphed quickly from primarily a strategic deployment capability into an enterprisewide fighting capability with shared target acquisition, air operations, red and blue (enemy and friendly forces) pictures and intelligence distribution. The operations tempo for the development of improvements surged to dozens of changes month to month, instead of the traditional rates of year to year.
- DISA's Defense Collaboration Tool Suite (DCTS) debuted early for real-time continental United States (CONUS) collaboration with forward-deployed component headquarters.
- Secure voice and video were pushed forward and made more "latency tolerant" to support theater operations.
- Theater-level, operator-friendly NetOps (network operations) applications were coded on the fly. The integration of leading commercial off-the-shelf tools with tailored and intuitive graphic user interfaces for the joint network operations (NetOps) manager was key to DISA's success in fielding several NetOps tools of choice: Network Traffic Analysis System (NTAS) and NETWARS, today known as Joint Com-

munications Simulation System (JCSS). Army Brigadier General Dennis Moran, director of command and control, communications, and computer systems at U.S. Central Command during the initial phases of OIF/OEF, stated, "For the first time, detailed theaterwide performance information is available to communicators across Southwest Asia, from my headquarters to the Theater Command Control Center Forward and the component commands in the Persian Gulf. This capability (NTAS) is being used daily to solve problems in the field and to keep senior leaders informed."

- Secure Iridium satellite phones instantly became one of the really good news stories in Afghanistan as the preferred link with the outside world and one's lifeline when all else failed. Rangers from the U.S. Army 75th Ranger Regiment said that during periods of Operation Anaconda in Afghanistan, "[Iridium] was our only means of communications out of the valley!"



DISA's Theater NetOps Center in Bahrain expanded to round-the-clock operations with six times the capability as pre-September 11. The DKET fleet continued to multiply to the point that 80 percent of the theater's bandwidth of nearly three gigabytes was met by commercial satellite service, as opposed to MILSATCOM. That is an inverse ratio to all previous major operations.

DISA and the military services met all preparatory NetOps milestones, so that all signal communications stoplights were green for the offensive operations on March 19, 2003. In the weeks of combat maneuver operations that followed, communications proved to be a force multiplier—not the C2 inhibitor that it had been in many previous wars.

The operations to defeat the Iraqi military forces were only the beginning of DISA's job in Iraq. Immediately following the initial offensive operations in Iraq, the assistant secretary of defense for networks and information integration tapped DISA to provide the DoD Office for Reconstruction and Humanitarian Assistance (ORHA) under Army Lieutenant General Jay Garner (Ret.) with Iraqi governance and re-

construction communications. The ORHA changed to the Coalition Provisional Authority (CPA) under Paul Bremer's leadership on May 11, 2003, and the main body took up residence in Baghdad's Republican Palace.

Over the next year, DISA's physical presence in Iraq surged to more than 140 military personnel, federal employees and contractors, who engineered and installed voice, data and video services throughout the CPA headquarters and Iraqi government buildings in Baghdad's International Zone, while under constant mortar and sniper attacks. DISA also became the primary cell phone service provider for U.S., Iraqi government and coalition personnel by installing a 10,000-subscriber network. With the dissolution of the CPA in July 2004, these DISA-fielded networks and services were "gifted" by DoD to the Department of State.

Early on, OEF highlighted the need for "big pipe" satellite reachback stations to support the vast array of new transformational, net-centric weapon systems. On the East Coast, four commercially operated gateways were added to the existing DoD teleports, quadrupling capacity. DISA beefed up satellite tactical entry point (STEP) sites across the board, particularly with Net Defense tools, making them high-capacity commercial gateways, as well as MILSATCOM gateways, to the global information grid. All in all, OEF preparations were a premonition of the even greater command, control and communications (C3) challenges to come.

In the summer of 2002, contingency planning for Operation Iraqi Freedom and the rapidly growing use of UAVs such as Global Hawk and Predator made it imperative that a thick robust GIG infrastructure be installed throughout the region. For starters, 17 high-capacity Defense KU-band Earth Terminal Systems (DKETS) were deployed with CENTCOM's Joint Deployable Force headquarters and regionally dispersed components. DISA was able to support the unprecedented DKET network, using the nine transponders leased previously, even though the media and international communities were arriving by the hords.

ONGOING COALITION WAR FIGHTING SUPPORT

DISA continued to improve the CENTCOM ICT infrastructure, expanding the satellite STEP and teleport capabilities and implementing a previously non-existent terrestrial, fiber grid throughout the region. The GIG's fiber connectivity in the region has grown exponentially from

Higher education and training are important aspects of sustaining a professional ICT work force in Iraq. In 2007, DISA designed and installed the first distant learning center for the College of Engineering at Salahaddin University in Erbil, Kurdistan Region. Shown here are United States Central Command Forces discussing final plans with University staff.

only two megabytes prior to September 11 to more than six gigabytes at this time.

Despite these huge improvements in the Central Region information and communications infrastructure, the forces within Iraq and Afghanistan remain almost entirely dependent on satellite bandwidth because of the lack of an international terrestrial infrastructure and painfully slow-emerging commercial services.

To address these deficiencies, the deputy secretary of defense in August 2006 established a new Task Force for Business and Stabilization Operations (TF-BSO) to accelerate the recovery of the Iraq economy, including ICT. The task force recognized the inherent need of every one of its planned initiatives for reliable communications.

The task force, including a DISA team, deployed to Iraq. Initially, DISA installed quick-fix VSAT (very small aperture terminal) communications packages (two-way, satellite ground stations with dish antennae) at isolated factories and local governance centers in the insurgency-riddled Ramadi and Diyala provinces. These governance and business-sector communications restoral efforts were important for the coalition force's counterinsurgency progress in the "secure-hold-build" phases of national stabilization and reconstruction.

Besides providing the government of Iraq with infrastructure technology expertise on specific improvements, there is assistance offered in helping develop a skilled Iraqi ICT work force. An example of this training and education goal is the distant-learning center that DISA planned and installed for the College of Engineering at Salahaddin University in Erbil, Kurdistan Region.

Concurrently, supporting the task force's strategic objective of commercial e-business and the Multi-National Forces-Iraq (MNF-I) need for efficient terrestrial bandwidth, DISA engaged with the Iraqi Ministry of Communications for reconstruction of its international gateway terrestrial architecture. In September 2008, these efforts resulted in the first operational DISA-leased fiber circuit with the Iraq Telecommunications and Postal Commission (ITPC). Additionally, under competitively awarded DISA contracts with private industry are additional fiber and microwave, terrestrial infrastructure and international gateways so that by spring 2009, the GIG's terrestrial fiber architecture should be extended into a robust Iraqi grid.

To complement its support for the TF-BSO reconstruction efforts, DISA deployed a second team called the DISA Support Element-Iraq (DSE-I) in January 2008 for Defense Information System Network (DISN) planning support to the MNF-I J6 (director of command, control, communications and computing). At the same time, TF-BSO transferred control of its DISA reconstruction team to the MNF-I J6 to facilitate the integration and synchronization of the

two ICT missions of supporting coalition forces and Iraqi reconstruction.

In February 2008, the MNF-I J6 established a team of experts to help improve coordination of communications policy, services and infrastructure initiatives throughout Iraq. The team, referred to as the Iraq Communications Coordination Element (ICCE), immediately focused on initiatives that leveraged the direct tie between ICT supporting the coalition forces and helping rebuild Iraq's capacity.

FUTURE COALITION WAR FIGHTING SUPPORT

DISA fully expects to remain engaged in an enduring need to improve the GIG infrastructure in the Central Region. Leveraging its lessons learned in Iraq, DISA is working closely with CENTCOM J6 to improve the ICT services in Afghanistan, particularly as the number of forces there will increase significantly over the next two years. Throughout the region, there are enormous, growing demands for real-time intelligence, surveillance, and reconnaissance (ISR) and for streaming video and imagery services. Information sharing and collaboration across all mission areas are expanding. These drive DISA to improve its GIG support and services.

Continuing improvements in the region's GIG infrastructure will focus on greater terrestrial fiber capacity and diversity; sustained satellite diversity with improved STEP and teleport gateway services; increased use at the tactical edge of digital video broadcast-return channel satellite (DVB-RCS), untethered, high-speed bandwidth support; better use of existing bandwidth with more fielding of GIG Content Delivery System (GCDS); full-scale implementation of cross-domain solutions; and improved end-to-end integration of network operations.

Building on its Iraq experience, DISA is preparing to deploy a DISA Support Element-Afghanistan (DSE-A) in the first part of 2009 for DISN planning support to the U.S. Forces-Afghanistan J6.

So what's the bottom line for DISA in support of OEF and OIF? Since day one, DISA has proven that its primary customer is the warfighter. Find the warfighter and you will find DISA. ★

DISA'S NETWORK SERVICES

DISA's Network Services Directorate is the single senior manager for the Defense Information System Network (DISN). Network Services translates customers' long-haul network requirements into effective voice/video/data network solutions. The directorate leverages proven and emerging technologies to ensure joint interoperability and provides assured security services for the Department of Defense's long-haul networks.

Network Services has several, very significant functions. The directorate:

- Plans, implements, sustains and evolves the Global Information Grid (GIG) networks; transport; special programs; and data, voice, messaging and video networks.
- Exercises responsibility for the Internet Protocol (IP) Core sustainment and life cycle management, Internet Protocol version 6 (IPv6), Voice over IP, the Network Information Center (NIC) and network operations centers.
- Designs, tests and implements enhancements to the DISN in support of GIG initiatives as an enterprise solution for the DoD and intelligence communities.
- Performs analysis and laboratory evaluation of advanced technologies to support insertion into the DISN.
- Provides network management and systems engineering, implementation and consolidation required by DISN and DoD's worldwide strategic and special-purpose circuit-switched networks.
- Plans, resources, implements, sustains and evolves Standard Tactical Entry Point (STEP) sites for the Defense Satellite Communications System in support of networks, computing services applications and information services.
- Provides management and technical assistance to DISN special projects and programs, which include DoD support to the direct communications links; deployment intelligence sharing among federal, state, local and foreign mission partners; DISN transition to the DISN Core; and DISN provisioning policies and process.
- Provides life cycle support for DISN data-

base systems and DISN access transport services.

- Manages DoD support to the Secret Service and special support to the Joint Staff Office of Special Events.
- Manages the Anti-Drug Network (ADNET) program in support of the Office of the Deputy Assistant Secretary of Defense for Counternarcotics and other counter-narcoterrorism mission partners.
- Sustains the Defense Message System (DMS), DoD's system of record for organizational messaging.

With so much responsibility and such a "full plate" of requirements, it is no surprise that the operational elements of Network Services had a very productive year in 2008, supporting DISA's customers. Network Services has 10 operational components: Data Services, Transport Services, Real Time Services, Voice Services, the Defense Red Switch Network, Video Service, DISN Transition Services, Customer Services, Operational Support Systems, and the Defense Messaging System.

DATA SERVICES DIVISION

In 2008, the Data Services Division completed transition of the Non-classified Internet Protocol Router Network (NIPRNet) IP routers onto the new DISN Core and made significant progress on the transition of the classified Secret IP Router Network (SIPRNet) IP routers. The division completed the Navy-Marine Corps Internet (NMCI) Phase II transition to NIPRNet and deactivated and removed old NIPRNet counterinsurgency (COIN) assets. In addition, Data Services completed Internet Access Point (IAP) bandwidth upgrades (seven circuits), nearly doubling the capacity for NIPRNet customers to access Internet, which had become saturated due to lack of bandwidth.

The division completed successful implementation of IP version 6 (IPv6) on NIPRNet, in accordance with DoD and Office of Management and Budget direction. The Data Services Division also completed a formal agreement with the American Registry for Internet Numbers (ARIN) for IPv6 address space allocation for DoD use. And the division migrated 10 Distributed Common Ground Systems (DCGS) program sites from the Defense Research and Engineering Network (DREN) to the DISN.

TRANSPORT SERVICES DIVISION

The Transport Services Division continued support to Operation Enduring Freedom, Operation Iraqi Freedom and the global war on terrorism in 2008. It sustained the global high-speed transport optical fiber infrastructure to support mission requirements; planned for the increase of trans-Atlantic bandwidth to support new requirements; continued replacing Promina multiservice access platforms for asynchronous transfer mode (ATM) with IP-centric technology; and completed fiber bandwidth upgrades in Southwest Asia. The division installed DISN core routers and additional transport at Al Udeid in support of a new tech control facility.

REAL TIME SERVICES DIVISION

In 2008, the division continued to implement the DISN IP Real Time Services (RTS) in the unclassified and classified IP transport wide area networks and continued modifying the DISN IP Core wide area network infrastructures to complement the development and implementation of specific RTS applications.

The Unified Capabilities Requirements (UCR) has been updated to the 2008 version (UCR 2008). RTS anticipates that it will be signed by the DoD CIO before the end of January 2009. After being signed, the UCR will become the authoritative document for voice, video and data over IP in DoD.

VOICE SERVICES

Among the significant achievements for the Voice Services Division during 2008 was the award of a contract for the addition of the assured services functionality in the transportable emergency response multifunction soft (ERMFS) switches. The division deployed one ERMFS switch to the Army in Southwest Asia and installed additional digital compression multiplex equipment in support of the Defense Switched Network (DSN) contingency operations in the U.S. Central Command area of operations. It completed the Unified Capabilities Requirements for 2008. The division also completed MFS upgrades in the continental United States (CONUS) and awarded a contract to upgrade Lackland Air Force Base and Scott Air Force Base to multifunction soft switches.

During 2008, DISN continued to exceed joint staff performance objectives in supporting the needs of the warfighter. During the past year, more than 202 million calls were made, lasting cumulatively for nearly 1.2 billion minutes. Included in those figures were 192,565 precedence calls.

DEFENSE RED SWITCH NETWORK

The Defense Red Switch Network worked on a number of projects in 2008, chief among them the deployment of a new generation of red switch secure voice equipment, sustainment of the Survivable Emergency Conferencing Network (SECN) and the Enhanced Pentagon Capability, improved reliability of service to mobile/transportable SECN systems. The division purchased replacement secure voice switches for two EPC/SECN sites. It completed fielding of the replacement telemetry system and backbone realignment and completed fielding of the expanded Voice over Secure IP (VoSIP) systems.

VIDEO SERVICES

DISN Video Services-Global (DVS-G) delivered 20,659,095 video-bridging minutes to more than 6,300 sites worldwide in 2008. The Video Division continues the transition to the next generation of video support, DVS-II.

DISN TRANSITION SERVICES DIVISION

During 2008, the DISN Transition Services Division continued CONUS transport circuit transitions at the rate of 30 circuits per week. The division continued DISN Transmission Systems-CONUS (DTS-C) transition onto the new DISN Core and onto the DISN Access Transition Services (DATS) contract and continued execution of CONUS Transport DTS-CE (CONUS Extension) circuit transitions at the rate of 20 circuits per week. Transition Services also completed the merger of NIPRNet/SIPRNet/GIG Bandwidth Expansion IP autonomous systems.

CUSTOMER SERVICES

In 2008, the Customer Services Division expanded the DISN Customer Call Center to a global operations contact center for all DISN services, supported GIG Waiver Panel decisions, conducted a DISN customer satisfaction survey, evaluated the use of commercial industry data standards for the DISN, conducted evaluations for improvement of provisioning processes and workflows, coordinated and published policies for last half-mile support and emergency maintenance procedures, created a communications plan for the DISN program, created a customer briefing to depict the DISN evolution, and published a strategy for DISN project management.

OPERATIONAL SUPPORT SYSTEMS

Possibly the most complex aspect of DISN evolution is moving the separate network management systems that exist today onto a common DISN Operations Support System (OSS). As the DISN evolved from separate networks and subsystems, the means of managing those networks and subsystems evolved relatively independently.

Progress has been made in moving service, network and element management onto a common OSS, but much remains to be done, including completing out-of-band management of DISN network elements and implementation of the Telecommunications Management Network (TMN) reference model as the basis for the new DISN architecture.

These steps are necessary to gain key operational, business and customer-service benefits, including rapid agile provisioning, policy-based management, consolidation of network operations, and improved levels of security and control. Enhancements will also be needed to manage a network where quality of service is based on statistical guarantees and policing of the “edge” vice nailed-up circuits.

During 2008, the Operational Support Systems Division completed Phase 1 of the service-oriented integration foundation for the Element and Network Management Systems (EMS) and consolidated the SIPR-Net network management to a single network management enclave. These efforts support our net-centric information-sharing capabilities and provide critical elements in support of DISN end-to-end situational awareness.

DEFENSE MESSAGING SYSTEM

The Defense Message System (DMS) Division in 2008 implemented enterprise guards to provide centralized, cross-domain support and continuously improved DMS operational performance and reliability. DMS Outside CONUS Tier I functions were consolidated to DMS Network Operations Center (NOC)-CONUS and now use the DISN Customer Call Center (DCCC) for the global DMS community. Assumption of Tier I network operations functions from the DMS NOCs at DISA-Pacific Field Office and DISA-Europe theater network operations centers (TNC) was successfully completed on November 28—two months ahead of schedule.

The transition enabled DISA to provide the global DMS community and the theater commanders with a single call center for all DMS issues while retaining theater visibility via the TNCs and the tactics, techniques and procedures (TTPs) associated with the DCCC and the DMS NOCs.

PACE CONTINUES IN 2009

There will be no slowing of the pace for Network Services in 2009. The need for the essential services provided by and functions performed by Network Services to enable routine and special communications throughout the world will continue unabated.



And in fact, the new year brought a special assignment to support the presidential inauguration on January 20. Network Services installed and maintained radio networks supporting Secret Service command posts and providing radio communications from the motorcade to the supporting command posts. In addition, temporary voice and radio circuits were provided in support of a number of multi-agency command centers (MACC) strategically positioned to support protection operations. Also, DISA had 30 technicians available to support as needed.

And the beat goes on! ☆

Final preparations are made prior to President-elect Barack Obama's swearing-in ceremony on the U.S. Capitol steps in Washington, D.C., Jan. 20, 2009. More than 5,000 men and women in uniform provided military ceremonial support to the presidential inauguration, a tradition dating back to George Washington's 1789 inauguration. [DoD photo by U.S. Air Force Master Sgt. Cecilio Ricardo]

GLOBAL INFORMATION GRID ENTERPRISE ENGINEERING

DISA's Global Information Grid (GIG) Enterprise Services Engineering Directorate (GE) plans, engineers, acquires and integrates joint, interoperable, secure, agile global net-centric solutions to satisfy the needs of the warfighter, and it develops and maintains a world-class engineering work force to support the agency's programs.

GE's core competencies include providing disciplined information technology end-to-end systems engineering; offering security expertise for the GIG; leveraging commercial off-the-shelf products and services to solve joint and coalition need; and swiftly delivering value-added, trustworthy, global net-centric solutions.



GE's operational elements are the Business Management Division, which acquires the necessary resources to ensure success of GE engineering missions, and two engineering centers.

The GIG Engineering Center provides functional network and communications engineering support and joint technical advocacy for DISA networks and for communications systems across the Department of Defense and the Executive Office of the President. The center also provides integration engineering support to DISA technical programs, ensuring interoperability with other developmental and legacy systems.

The Systems Engineering Center provides world-class systems engineering and end-to-end analytical support for DISA and its customers, ensuring integrated capabilities in support of warfighter mission requirements.

GIG ENGINEERING CENTER (GE2)

The GIG Engineering Center comprises four divisions. The Network Engineering Division provides engineering support to the Defense Information System Network (DISN) and for gateway functions for satellite communications (SATCOM) and tactical networks. The SATCOM Engineering Division serves as the systems engineer for SATCOM, providing technical assistance and joint advocacy for SATCOM systems across DoD.

The Strategic Communication Division provides technical leadership for communications systems serving DoD nuclear command and control, the national military command system, missile defense systems, senior leadership airborne command and control systems, and support for White House conferencing systems. Finally, the Integration Engineering Division ensures that technical solutions that are being developed across the agency are integrated and compatible both with each other and with legacy systems.

The Network Engineering Division provides the primary engineering support to the DISN, both for operational issues and future development. A primary focus for 2008 has been migrating disparate legacy networks onto the new DISN optical core transport network, and where possible converting them to native Internet Protocol.

Notable successes include the engineering design work necessary to support DISN transport technical refresh efforts, the classified Secret Internet Protocol Router Network (SIPRNet) aggregation router transition, and new non-classified NIPRNet Internet Access Point connection designs. (Previously, IP routing was fragmented across several systems—none capable of advanced routing such as multi-protocol label switching, virtual private networks, and quality of service, all of which are critical warfighter needs.)

In addition, the Network Engineering Division supported the design and development of the Joint IP SATCOM Modem, enabling the interface of SATCOM networks with the DISN IP networks. (Previously, all SATCOM was point-to-point, static bandwidth allocations. With the Joint IP Modem, SATCOM will be able to be dynamically managed with bandwidth-on-demand and will automatically share IP routing information with the terrestrial networks.)

The design work for future DISN transport required that the division first develop a comprehensive network-evolution strategy that laid out a detailed engineering road map for how the DISN would converge legacy non-IP networks to IP and then migrate them to the new DISN IP core. The vision for the next 10 years was successfully developed, resulting in both approval

U.S. Army 1st Lt. Jason Behler speaks to his soldiers via a two-way radio while searching for a known weapons trafficker in the Jihad community of southern Baghdad, Iraq, Dec. 23, 2008. Behler is assigned to the 4th Infantry Division's Company C, 1st Battalion, 22nd Infantry Regiment, 1st Brigade Combat Team.
[U.S. Army photo by Sgt. David Hodge]

of more than \$60 million in additional near-term DISN funding for technical refresh of the IP transport equipment and in the selection of the DISN as a provider of wide area network transport services for the Navy's upcoming Navy-Marine Corps Intranet (NMCI) Next-Generation network (NGEN).

The Navy will leverage the existing DISN transport infrastructure, net-centric enterprise services, defense enterprise computing centers, and network operations capability. This will be a significant step toward DoD establishment of a true information enterprise capability, and will enable significant cost savings when compared to the costs of the current vendor-provided networks that support NMCI.

The SATCOM IP modem technology pioneered by the division as the engineering support for the Global Broadcast System and the Direct Video Broadcast-Return Channel Satellite (DVB-RCS) network led directly to the decision to procure a joint IP modem for use throughout DoD. The DVB-RCS network was originally developed as a short-term solution for collection and broadcast of Predator and other unmanned aerial vehicle video throughout the Iraq and Afghanistan combat theaters.

The technology was successfully developed and deployed by the Network Engineering Division on a short schedule, and quickly became a mainstay for operations Iraqi Freedom and Enduring Freedom. The effort, which began in fiscal year 2007, tripled in size during fiscal year 2008. Primary users are Multi-National Coalition-Iraq, the Air Force Predator Program Management Office and U.S. Army Task Force-Oden.

The SATCOM Engineering Division collaborated in the Joint IP Modem development, and also made great strides toward fielding the Integrated Waveform (IW). IW provides enhanced ultra-high-frequency (UHF) SATCOM demand-assigned multiple access (DAMA) capabilities with improved efficiency and quality of communications. IW increases the number of accesses 240 percent—from five to 12 2,400-bits-per-second networks over a 25-kHz channel. This translates to an increase of several hundred networks for tactical SATCOM users.

Additionally, IW provides improved link margin, increased voice quality and simplified setup procedures. Currently three UHF SATCOM radio vendors are under contract to deliver IW software: Harris for the PRC-117F, Raytheon for the PSC-5 and ViaSat for the MD-1324 and IW Controller. GE has successfully tested IW over the air and demonstrated the new capability at the DISA Customer Partnership Conference.

The SATCOM Engineering Division additionally supported DoD SATCOM analyses for the Transformational Satellite Communications System (TSAT) PDM-II study, advanced extremely high frequency (AEHF) Nunn/McCurdy certification, Information Transport Functional Solutions Analysis, SATCOM Gateway analysis, and other enterprisewide requirements analyses. The analyses included detailed examination of warfighter requirements, satellite capacities, and SATCOM terminal availability for certain scenarios and time frames.

DISA and U.S. Strategic Command (USSTRATCOM) jointly signed the SATCOM-GIG Integration Vision and Strategy. The vision and strategy were jointly developed by USSTRATCOM and DISA, along with broad stakeholder support. Long operated as a separate entity with its own unique management systems, DoD SATCOM must be integrated into the GIG network operations (NetOps) framework to efficiently use scarce DoD SATCOM resources and effectively perform end-to-end GIG NetOps. The need for this vision and strategy is particularly important because of the launch of the first Wideband Global SATCOM (WGS) satellite in October 2007, as well as future WGS launches, AEHF-protected satellites, Mobile User Objective System (MUOS) narrow-band satellites and TSAT satellites.

The Strategic Communications Division, acting for the DISA director in his role as the nuclear command, control and communications (C3) systems engineer, provided exceptional support to Office of the Secretary of Defense (OSD), Joint Staff, USSTRATCOM and other nuclear commanders by instituting "mission stream" realism in operational assessments—providing certification recommendations for several vital nuclear C3 systems—and documenting and updating authoritative nuclear C3 engineering, architecture and program documents.

Under presidential direction, the division also provided and assisted in the installation of two overseas head-of-state, secure video-teleconferencing systems; completed 12 installations and upgrades of the Crisis Management System (CMS), including improvements on executive aircraft; and began expansion of the executive voice-over-secure IP network in 2008.

The division completed engineering and installation of the NORAD Contingency Suite (NCS) in the National Military Command Center, completed analysis of Enhanced Pentagon Capability (EPC) HEMP facilities, and developed an EPC maintenance plan to help site managers keep their EPC installations functionally viable.

During 2008, DISA GE2 completed the design of very-high-availability, DISN-based inter-site connectivity for the Missile Defense Agency's (MDA) Ground-Based Midcourse Defense (GMD) weapon system. DISA will implement this connectivity between GMD sites in 2009, with MDA transitioning GMD long-haul communications from a proprietary vendor network to the DISA-provided infrastructure and network operations in 2010. This transition will result in a multimillion-dollar savings to MDA and DoD, by eliminating the need to separately contract for proprietary vendor services that can be provided more cost effectively by DISN.

The Integration Engineering Division works across DISA programs and projects to increase interoperability and reduce redundant development efforts. One specific area of success in 2008 was the work done by the division to champion the concept of Policy-Based Enterprise Management (PBEM) across the agency. PBEM will benefit network management work being done by DISA Network Services (NS), GIG Enterprise Engineering, GIG Operations, and across DoD. Concept demonstrations to DISA senior leaders and at the DISA Customer Partnership Conference were a great success and showed the value of this technology to GIG NetOps.

Since these demonstrations, requests from both inside and outside of DISA have been received. DISA's Net-Centric Enterprise Services (NCES) and Net-Enabled Command Capability (NECC) program executive offices (PEOs) have expressed interest in applying this technique to capability modules for establishing a common service-oriented architecture (SOA) and to the redirection of command and control (C2) services.

In addition to those specific projects discussed above, GE2 is supporting the DISA Center for Network Services on the Real Time Services (RTS) pilot; working with PEO-IAN (Information Assurance and NetOps) and the Joint Task Force-Global Network Operations (JTF-GNO) on the potential application of "white list filtering management"; and exploring a partnership with the Air Force, Navy and Army to leverage this technology for airborne and tactical environments. GE2 has generated interest in both government and industry to participate in the Tele-Management Forum's Defense Interest Group in order to support the development of standard-based products and interfaces.

SYSTEMS ENGINEERING CENTER (GE3)

The Systems Engineering Center is organized into three divisions: the End-to-End Systems Engineering Division, the Interface Standards Division and the Modeling and Simulation Division.

The End-to-End Systems Engineering Division provides support both to internal DISA programs and to the rest of DoD, working through the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) to provide enterprisewide systems engineering and Internet Protocol version 6.0 (IPv6) transition planning and assistance by staffing the DoD IPv6 Transition Office.

Key accomplishments related to internal DISA programs for 2008 included reviewing and assessing more than 340 programmatic documents as well as the maturity and technical readiness of more than 45 programs; sponsoring the creation of a course by the Defense Acquisition University on how to develop a systems engineering plan, of which two classes were conducted in fiscal year 2008 with 47 attendees; and conducting systems-engineering plan development workshops with representatives from 29 DISA program

offices attending. Finally, the division conducted an architecture gap analysis of DISA Acquisition Category (ACAT) I and special interest programs against the Defense Information Environment Architecture.

In support of the ASD (NII) enterprisewide systems engineering (EWSE) efforts, the End-to-End Systems Engineering Division completed a series of requested technical tasks that concentrated on the tactical environ-

ment. This included the development of a service-oriented architecture for the tactical environment, as well as an enterprise management approach for tactical networks. The division also developed a concept for a Border Gateway Protocol-based High Assurance Internet Protocol Encryption (HAIBE) peer discovery service, allowing encrypted traffic to be correctly routed at the tactical backbone.



U.S. Air Force Airman 1st Class Justin Iverson conducts a patrol in the Doura district of Baghdad, Iraq, Nov. 22, 2008. Iverson is assigned to Detachment 3, 732nd Expeditionary Security Forces Squadron, attached to the 1st Brigade Combat Team, 4th Infantry Division.
[U.S. Navy photo by Petty Officer 2nd Class Todd Frantom]

The End-to-End Systems Engineering Division also stepped up outreach efforts to the department to enhance interoperability and cooperative capability development by providing support to the Joint Tactical Radio System (JTRS) Program Office, the Joint Staff for Joint Basing and GIG 2.0 efforts, and the Naval Research Laboratories. The division established an EWSE wiki site to further enable cooperative EWSE efforts.

During 2008, the division worked to manage the transition of the department to IPv6. The DoD IPv6 Transition Office developed and submitted to OSD the Congressional DoD IPv6 Integrated Implementation Schedule and an IPv6 Test and Evaluation Report. One important achievement was the development of an IPv6 addressing plan, which required working with experts from the division, throughout DISA and across DoD. In completing the schedule and report, the division achieved the following successes:

- Submitted DoD test and evaluation report to Congress early.
- Met DoD's IPv6 requirement for the GIG, as mandated by the Office of Management and Budget.
- Coordinated with DoD to advance Joint Staff IPv6 criteria.

The Interface Standards Division is responsible for managing the information exchange and communications standards for DoD, and it maintains the DoD IT Standards Registry (DISR). The division also represents DoD in the development and approval of national and international information exchange and communications standards. Key work was done in 2008 on the standardization of core architecture data models, including international participation on the production of an Open Office Extensible Markup Language (OOXML) standard. The division successfully promoted the GIG technical guidance as a reliable mechanism to identify requirements for building or accessing GIG capabilities.

The division also sponsored the development of a Common Terrorism Standards Registry (CTSR). By providing the technical expertise to create a registry, the Interface Standards Division supported the distribution of terrorism information and suspicious activity reports across the federal, state, local and tribal law-enforcement and civil-defense authorities.

An additional successful effort was the transitioning of the updating of two joint tacti-

cal communications manuals (CJCSM 6231.03-Joint Data Systems and 6231.05-Joint COMSEC) to a wiki site under Army sponsorship. This will enable these manuals to be continuously updated with the most current technical data by experts in the field.

The Modeling and Simulation Division provides support to DISA Network Services (NS) and programs across DISA needing prediction and analysis from computer-based modeling. The division supported the DISN requirements for transport layer modeling to support technical refresh efforts, SIPRNet aggregation router transition, new NIPRNet Internet access point connections, and consolidation of legacy network traffic onto the IP backbone. This provided status for the traffic flow of information, which has helped DoD design and expand the communications services. In addition, it serves to protect DoD information systems.

In 2008, the division contributed to a successful Milestone C decision (the acquisition program milestone that moves a program into the production and deployment phase) for the NCES program by conducting performance and scalability tests of the NCES collaboration service. These modeling efforts aid the engineering and planning efforts and ensure that implementation proceeds smoothly without any adverse customer impact.

The division also monitored and analyzed network operations between the Internet and the DISN, providing data used by the JTF-GNO for decisions to manage Web traffic and to control access. The completed Internet usage analyses, in conjunction with information provided by Network Services and JTF-GNO, were used for House Armed Services Committee briefings on the topic of Internet blocking and for the director's "for government use only" proposal to ASD (NII).

In 2009, GE3 will be focusing on expanding engineering analysis in support of DISA efforts, such as NCES, PEO-IAN, GIG Operations and JTF-GNO, as well as establishing a software systems engineering and architecture capability and improving our enterprisewide systems engineering process and products.

2008 was a very busy and productive year for GIG Enterprise Services Engineering Directorate, and 2009 promises to be "bigger and better." ★

NET-CENTRIC ENTERPRISE SERVICES

The Department of Defense is transforming the way it conducts warfare, business operations and enterprise management. As a part of this transformation, DoD has embraced the concept of net-centricity.

Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes and people) in which data is shared in a timely and seamless way among users, applications and platforms during all phases of war fighting efforts. Net-centricity substantially improves situational awareness, significantly shortens decision-making cycles and provides better asset protection.

The Global Information Grid (GIG) Enterprise Services Program Executive Office (PEO-GES) in DISA has been charged with the responsibility to provide executive life cycle management of enterprise capabilities to support the DoD transition to net-centricity. PEO-GES provides oversight in planning and delivering enterprise services and support to mission performance across the warfighter, business and intelligence mission areas. The PEO is working through the Net-Centric Enterprise Services (NCES) program to extend enterprise services throughout DoD and to provide timely and accurate information to the warfighter anywhere and anytime.

NCES is the DoD-wide initiative to develop shared underpinning capabilities and provide foundational components for a secure, collaborative information-sharing environment with unprecedented access to decision-quality information. As a key enabler of the DoD Net-Centric Data Strategy, NCES is one of the catalysts to enable DoD's transition to an environment where all data is tagged and rapidly searchable by authorized users and applications.

NCES comprises commercial products and standards designed to connect users and computers with relevant information. NCES includes four product lines providing enterprisewide managed services: Collaboration, Portal (user access), Content Discovery and Delivery, and Service-Oriented Architecture Foundation.

FROM CONCEPT TO PRODUCTION

DISA has been working hand-in-hand with the operational sponsor at U.S. Strategic Command (USSTRATCOM) to ensure that NCES capabilities are responsive to war fighting requirements. As a result,

the NCES program successfully achieved Milestone C on June 13.

The Defense Acquisition Management Framework provides an event-based process through which acquisition programs proceed through a series of milestones associated with significant program phases. Achieving Milestone C is an indicator that the system-level technical requirements have been demonstrated to be adequate for an acceptable operational capability, and it provides entry into the production and deployment phase of the acquisition life cycle. The purpose of this phase is to achieve an operational capability that satisfies mission needs. Operational test and evaluation will determine the effectiveness and suitability of the system.

Several important documents that pertain to the product support, which includes strategy, performance and funding, were required to achieve this key milestone. PEO-GES is an active participant in the working-level integrated product team—along with the Office of the Deputy Under Secretary of Defense for Science and Technology, Office of the Assistant Secretary of Defense for Networks and Information Integration, Operational Test and Evaluation (DOT&E), Program Analysis and Evaluation, USSRATCOM as the operational sponsor, and an extensive list of user organizations—which delivered the required program documentation and memorandums of agreement, resulting in the successful entry into the production and deployment phase.

In parallel with the acquisition-related activities, the program made great strides demonstrating and testing the net-centric solutions via its four product lines. The innovative approach for testing, conducting testing of modules in early user tests (EUT) aligned with the product line development schedule, enabled NCES to achieve limited operational availability (LOA) for NCES Spiral 2.0 capabilities in May. DOT&E approved the NCES Test and Evaluation Master Plan (TEMP) in May. The LOA designation allowed the user community to use the NCES services prior to achieving full production capacity.

CONNECTING USERS ON THE NETWORK

Making the NCES services available to the user as they completed EUT provided an opportunity to evolve the capabilities based on user feedback and lessons learned. The most notable accomplishments during the year included:

- The Defense Knowledge Online Portal implemented automated account provisioning for all DoD active/Guard/Reserve military and civilian personnel on July 2.
- The NCES collaboration and portal capabilities were used during the Democratic National Convention August 25–26 to share information and collaborate.
- Key Federated Search and Enterprise Catalog capabilities were brought online on the NIPRNet in August.
- The enterprise file delivery capability was used to deliver more than 1.2 terabytes of data to support the global war on terror.
- The GIG content delivery service on the Secret Internet Protocol Router Network (SIPRNet) was used to deliver 1.5 terabytes of content faster and more efficiently to more than 175,000 users.
- The NCES collaboration service was recognized by Computerworld as an Honors Program “Laureate” for 2008.
- The NCES Net-Centric Publisher was implemented on the SIPRNet and the non-classified NIPRNet in September, providing developers a single point of entry into the NCES environment.



ability of the war fighting, business and intelligence mission areas to better share information and respond to joint network operations and missions. Leveraging the early work accomplished by the NCES program and the intelligence community, the ESERB endorsed a Service Security Reference Architecture and associated interface specifications as a recommended best practice.

The ESERB is currently addressing standards and best practices for several of the enterprise service areas, including collaboration, service discovery and content discovery. This governance forum and its members and associated working groups

are key contributors to defining a set of common standards, specifications and reference implementations to enable joint interoperability.

NEXT STEPS

Expanding on a strategy to conduct EUTs and continuously monitor usage in concert with the test community, the program and test agencies are working with programs of record to conduct an initial operational test and evaluation (IOT&E) in accordance with the TEMP. The modular approach for testing being applied to the IOT&E provides the flexibility to align the test events with the program capabilities and lays the foundation to become a best practice for testing net-centric applications.

The IOT&E is expected to take place throughout the remainder of the year. Initial operational capability is expected in April 2009. NCES full operational capability is scheduled for March 2010. ★

SHARED GOVERNANCE

PEO-GES was a leader and active participant in establishing the Enterprise Services Engineering Review Board (ESERB). The board’s mission is to provide a forum for establishing systems engineering management and oversight over key technical standards, specifications and reference implementations. The ESERB is co-chaired by the PEO-GES and a representative of the Office of the Director of National Intelligence (ODNI). The board includes representatives from across DoD and the intelligence community.

This body ensures that DoD and the ODNI implement enterprise services that improve the

U.S. Marines with 5th Battalion, 10th Marine Regiment learn how to operate Humvee Egress Assistance Trainers at Camp Wilson in Twentynine Palms, Calif., Jan. 5, 2009. (DoD photo by Lance Cpl. Charles S. Howard, U.S. Marine Corps)

RACE AND CLOUD COMPUTING

DISA Computing Services provides world-class processing capability, systems management, communications and storage in support of Department of Defense military services, agencies and combatant commands. Located in 18 secure facilities strategically placed throughout the world, our computing services support more than 3 million users of more than 14,000 applications using more than 1.7 petabytes of storage. Computing Services has become DoD's number-one provider of personnel, payroll, logistics, accounting and medical records processing.

Major areas of DISA Computing Services are resource management, customer management, operations, logistics, infrastructure management, lines of business and the Defense Enterprise Computing Centers.

This article focuses on one of the newest initiatives of Computing Services—Rapid Access Computing Environment (RACE).

RACE is the first service offered by DISA to address cloud computing. In most networking diagrams, “the cloud” refers to the Internet. It is ambiguous space; the user has no need to know the path that information follows, or what servers, nodes and paths the connection makes. Cloud computing builds upon that concept. The user “rents” space (a server, computing machine, software and so on) from a provider, but doesn't necessarily have a specific box or location. In other words, the user isn't purchasing a computer; the user is purchasing the ability to compute. All of what goes on “in the cloud” is invisible, by design, to the user.

RACE is a quick, low-risk, secure solution for developers, testers and anyone who needs a computing environment. Using a credit card or a Military Interdepartmental Purchase Request (MIPR), a user can purchase a basic computing environment. This is a process that, at one time, could take months. Building on DISA's capacity service contracts, along with industry partnerships, RACE reduces the time to just 24 hours.

DISA's foray into cloud computing originated with a request from then-director Air Force Lieutenant General Charles E. Croom Jr. for agile computing. With RACE, users have the ability to sign onto a portal, view a list of service offerings, design their environment, and purchase the service with a credit card or MIPR. Within 24 hours of funding approval, the user will have a computing environment.

“RACE will provide a fast, secure, and flexible environment for the user,” said Air Force Colonel Joseph Means Jr., RACE's program manager through development and initial deployment. RACE is agile indeed.

FLEXIBILITY, SCALABILITY, ECONOMY

RACE uses virtual server technology to scale capacity up or down based on user demands. In computing centers in the past, as many as half of the servers in operation could be used at as little as 10 percent capacity. Virtualizing servers, creating numerous virtual computers on a single box, allows servers to be used more efficiently, thus reducing costs.

In addition to the program being able to scale rapidly allowing it to support customer demand, individual users can scale their environment to suit their individual requirements. If a user has requirements beyond the initial package, they can simply add more capacity using the self-service portal.

Users purchase an environment on a month-by-month basis, so the costs and risks of acquiring and sustaining a computing environment are mitigated. The base price for service is \$500 per image. When a user is done using the environment, the computing resources are returned to the pool.

DEVELOPERS, START YOUR CREDIT CARDS

The ability to quickly purchase a computing environment using a credit card is a revolutionary advance in agility for DoD. The credit card transaction is basically instantaneous. A customer can use a credit card for the first month of provisioning, and then use an MIPR to provide funding as required to continue using the platform. This allows a customer to get a quick start and to continue to fund in whatever way is most convenient.

Another benefit of the ability to purchase the service with a credit card is accessibility, both to government personnel and contractor partners.

“We've tried to keep this as accessible as possible, to both government and to our contractor-partners,” said Steve Kerr, RACE program technical lead.

Access security is provided via public key infrastructure (PKI) credentials contained on users' common access cards. Allowances for “soft certs,” credentials that are provided by various certifying authorities who are recognized by DISA, are available for users who do not have a CAC.

MORE SECURITY

RACE provides a gateway to the Defense Enterprise Computing Centers (DECCs) and will reinforce DoD security standards. The RACE pilot will initially reside in a DECC Zone B enclave. Different enclaves have differing levels of security; Zone B provides security levels appropriate for development and testing.

One beneficial by-product of customers using RACE is that it will encourage the use of a standard operating environment and will thus promote a standard architecture across the department—a benefit leading to increased interoperability and decreased stovepipes.

FUTURES

Initial-operational-capability testing for RACE started with DISA's Computing Services Directorate in August 2008. RACE was deployed to customers in October, the beginning of the new fiscal year. Meetings with customers and potential customers have helped DISA staff prioritize upgrades to the RACE environment. Additional storage capacity and backup capabilities are first on the list for fiscal year 2009. Adding the Solaris operating system to the menu is another high priority.

Security certification and accreditation (C&A) concerns from customers have emphasized the need to establish a process and procedures that

will guide users through the C&A structure, simplifying and organizing all the required steps. DISA will be working with the appropriate security representatives to implement these processes.

RACE begins to address the capabilities of the cloud computing concept; however, anticipated offering beyond the pilot include providing access to an environment supporting pre-production testing with appropriate security, known as a Zone A enclave; software and services, including applications, utilities, Federated Development and Certification Environment (FDCE) design tools, and security services; higher capacity servers with additional optional storage; backup and continuity of operations (COOP) capabilities; and additional operating systems. ★



PROTECT YOUR CLASSIFIED HARD DRIVE. FORGET THE LOGISTICS.

NO SAFE, NO COURIER SERVICE, NO HASSLE.

Ensure the protection of your classified and sensitive unclassified data and avoid logistical hassles by securing your computer's hard drive with an Inline Media Encryptor (IME) from ViaSat. ViaSat's **KG-200** and **KG-201** IMEs are the first NSA-certified Type 1 media encryption devices that protect classified data-at-rest (DAR) at Top Secret (TS/SCI) and below, eliminating the need to courier your classified hard drive when transporting or locking it in a safe when not in use. Simply remove the IME's Crypto-Ignition Key (CIK) to quickly and easily secure your hard drive with your data encrypted.

TEL 888.ViaSat.1
EMAIL insidesales@viasat.com
WEB www.viasat.com/secure-DAR



Copyright © 2009 ViaSat, Inc. All rights reserved. ViaSat and the ViaSat logo are registered trademarks of ViaSat, Inc. All other trademarks mentioned are the sole property of their respective companies.



KG-201

» FOR PORTABLE USE



KG-200

» FOR WORKSTATIONS

GIG 2.0: THE NEXT BIG WAVE

DISA's chief information officer and chief technology officer agree: The Department of Defense and the agency can learn a thing or two from the technology that powers such commercial industry giants as Amazon, FedEx, Google, OnStar and UPS.

During a discussion on the value of using commercial technology to realize the Department's Global Information Grid 2.0 vision, John Garing, chief information officer and director of strategic planning, and David Mihelcic, chief technology officer, believe that the agency can and should do more to ensure that DoD has the latest and greatest technology to carry out countless missions. GIG 2.0 may be the answer to DISA's next-generation technology.

Mihelcic summed up GIG 2.0 as DISA's effort to harness Web 2.0 approaches and technologies "to do the things we want to do at the Department of Defense, such as collaboration, data-sharing and being able to make better decisions more quickly."

He cited user participation, openness and network effects as being especially relevant to DoD and DISA's IT needs.

"Those three things—user participation, openness and network effects—are what we have been talking about for years at the Department of Defense, with this notion called net-centricity and the GIG itself," Mihelcic said. "We want to expose information as broadly as possible. We want to move from this need to know to a right to know or need to share."

Mihelcic said that DISA's ability to connect more people to the GIG will mean a broader level of information-sharing, which in turn will mean better collaboration and better capabilities for the military.

According to Garing, DISA can get technology into the hands of warfighters at a much more rapid pace by continuing to adapt existing technology for DoD application, which is a goal that was championed by recently retired Air Force Lieutenant General Charles E. Croom Jr., who served as DISA's director from July 2005 to July 2008.

"I think that young people today have an unquenchable thirst to collaborate and share information," Garing said. "We have to get agile enough that we can adopt these systems as they evolve in the marketplace and take advantage of their power."

An example of this, Garing said, is that social networking can also be used to benefit military personnel who transfer from one duty station to another—called a permanent change of station or PCS. Personnel can research their new location to learn about installation facilities and services, family programs or available medical care.

Garing said that existing technology can be adapted to meet the needs of the military. He cited UPS's Delivery In-

formation Acquisition Device (DIAD)—the handheld computers that their drivers carry. The device instantly passes package and delivery information between the driver and UPS data centers, and using built-in Global Positioning System (GPS) technology, it enables UPS to continually track the location of the driver.

"I like the concept of the DIAD. UPS knows where every driver is, every minute of every day, globally," Garing said. "The DIAD just works."

While that particular device may not be practical in its current form for use in a combat zone, Garing said that the commanders on the ground could make the determination of how similar technology could be deployed in a secure manner and used for tactical purposes.

Garing, Mihelcic and other DISA leaders have spent time meeting with industry leaders and observing their commercial innovations to determine if and how these innovations are applicable to military functions and requirements.

For instance, Mihelcic said that he uses a well-known Web-hosting service—GoDaddy.com—that he believes could serve as a model for what DISA is attempting to accomplish for its customers. He has urged Alfred Rivera, director of DISA's Computing Services Directorate, to implement a similar system that would match the service in speed and price. Mihelcic dubbed the proposed DISA version of the service "GoAlfred.com" after Rivera. Rivera's response has been the development and deployment of the Rapid Access Computing Environment.

"The single most important thing that DISA can do is to provide a computing platform that takes the burden of the complexity of servers away from the customers," Mihelcic said.

"It [the computing platform] would be flexible and provisioned based on the user's needs," Garing added.

Following a tour of OnStar Corp., Garing envisioned a similar system throughout DoD that would allow tracking and diagnostics for every government vehicle. He noted that the OnStar call center is readily available at the push of a button.

"Just think of the money DoD could save if we could use a centralized diagnostic [system], which OnStar offers, for the government vehicle fleet," Garing said.

Mihelcic said that DISA's forward thrust into GIG 2.0 is happening today, rather than three years down the road.

"This stuff is happening every single day," he said. "Community and collaboration are a big part of that [GIG 2.0]."

Garing, recalling Croom's ABC strategy of "adopt before buy and buy before create" and philosophy that delivering a less-than-perfect solution fast was better than waiting years to perfect a solution, said that DISA is not ashamed of taking less than 100 percent.

"We'll take what we can to get it to the field fast and use it," he said. ★

THE CHALLENGES OF INFORMATION ASSURANCE

Department of Defense experts in information assurance are diligently seeking ways to provide wireless, mobile capabilities, including voice and e-mail, for classified and unclassified networks without compromising the essential elements of information assurance: authentication (ensures users and information are genuine), confidentiality (preventing disclosure of information to unauthorized users), integrity (data cannot be altered by unauthorized users), availability (information, computing systems and security controls are available when needed), and non-repudiation (a control ensuring that the sender cannot deny having sent a transaction and the receiver cannot deny having received it).

SECURITY OF THE NETWORKS

The need for information assurance increases every day for the Department of Defense. To foster faster development of a more secure Global Information Grid, DISA is collaborating with other DoD, federal and industry partners to improve information security for the department.

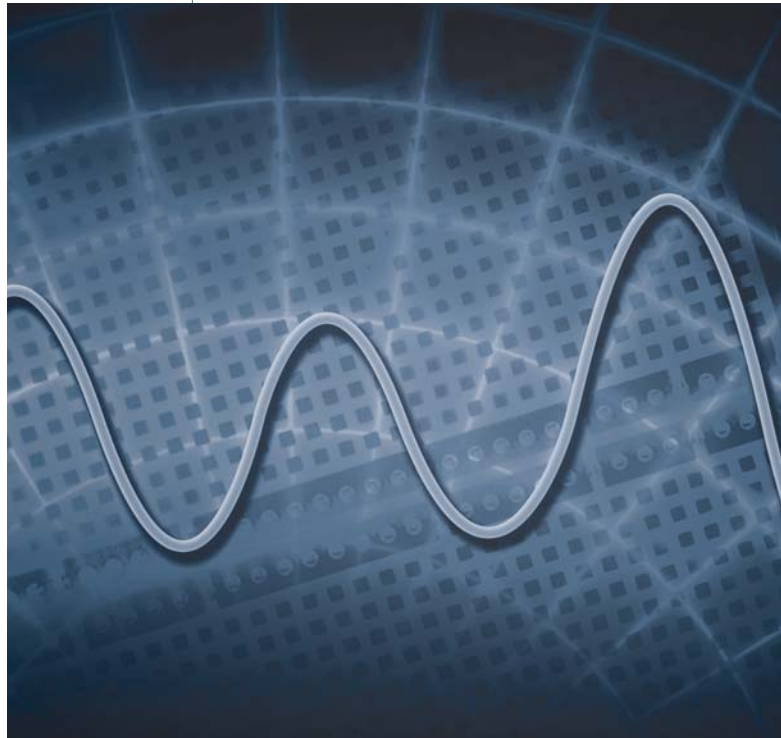
An important initiative to DISA is to strengthen the control of devices that are allowed to connect to the classified Secret Internet Protocol Router Network (SIPRNet). DISA is working with the military services to deploy a technology called network admission control (NAC) as a means of authenticating devices, not just people.

“We will combine this with an upgrade to the DoD public key infrastructure (PKI), which will issue identification credentials for devices,” said Mark Orndorff, DISA’s program executive officer for information assurance and network operations. Admission control is another layer of protection on the SIPRNet and leverages existing relationships and technologies.

A related effort is to strengthen the cyber-identity credentials DISA issues to people who use the SIPRNet. DISA has teamed with the National Security Agency

(NSA) to upgrade the SIPRNet PKI from a software-only credential to issue PKI credentials on a hardware token, much like those on a Common Access Card, which is currently used to authenticate people on the unclassified network.

“We’re working another effort to improve the individual authentication controls on the SIPRNet, taking the capabilities we have with PKI and mirroring that on SIPRNet,” Orndorff said. “Basically we are strengthening the way we make sure that our SIPRNet is allowing only connections to things that we want—that we’ve authorized—to connect to.”



CONFIGURATION STANDARDS

Configuring every device in the information infrastructure is essential. DISA is a part of a large-scale federal initiative to define configuration standards. Along with NSA and the National Institute of Standards and Technology (NIST), DISA publishes configuration guides for many technologies used by DoD and other agencies.

“We’re focusing a lot of attention on improving the configuration standards throughout DoD. That’s basically a fundamental principle; we have to have clearly defined security configurations that we consistently apply across all of DoD,” said Orndorff.

“There are about 7 million devices with Internet Protocol addresses on the unclassified network. Getting them configured correctly, keeping them configured correctly and measuring them is an enormous challenge given the incredible diversity of DoD’s mission and the incredible mobility of DoD. We are far more mobile than any other large organization in the world,” said Richard Hale, DISA’s chief information assurance executive.

“To help our DoD customers deal with this complexity, we are trying to drive as much automation as possible into the configuration process. As part of this, we’re also trying to drive toward standardization of the data involved in the business of configuring correctly, keeping things configured correctly, and measuring that they are configured correctly,” said Hale.

“We’re participants in a government/industry effort led by the National Institute of Standards and Technology called the Security Content Automation Protocol, which is defining standards for describing a configuration, defining measurements of the configuration, naming and describing vulnerabilities, and the like,” said Hale. In order to be successful, this government/industry team must also work the challenge of how to maintain a configuration as technology advances.

“This is one of the reasons why we are participating in these major standardization efforts—to try to improve the automation,” he said, which in turn increases the overall security.

WIRELESS SENSOR GRID

The convenience of home wireless technology is an incentive for employees to connect to the enterprise unclassified network from home using a small office/home office-grade access point to connect to a local access network. Whether unintentional or intentional, this act punches a hole in the enterprise security system, exposing critical data to those who would ordinarily not have access to the enterprise and compromising the network.

In an effort to thwart the consequences of rogue access points, DISA has traditionally attacked the issue twofold: the scanning of hardware and software and remediation. Scanning involves checking everything from the local enclave level to the entire architecture for vulnerability. Remediation deals with pushing out patches on the server and workspaces.

Recent work conducted by the Computer Network Defense Enterprise Solutions Steering Group has yielded results that will be the footprints toward a wireless sensor grid that will be a more holistic approach to detecting these connections. These results, upon scrutiny, will provide insight

into the maturity of current technology to determine whether it has matured to such a level that funds can be dedicated to this initiative.

“This is where I think we want to go in the long run,” said Orndorff. “We don’t have firm specific plans right now. We’ve gathered the plans from industry; now we’re going to take a look at it and decide whether we put money there or not.”

GROWING PAINS

Over the past several years we’ve worked to put capabilities in the hands of systems administrators.

“We provide tools to help to harden the operating systems—to harden the hosts. We have host-based intrusion detection, host-based intrusion prevention, vulnerability scanning and vulnerability remediation as products we directly acquire and provide for the military services,” Orndorff said. Putting these tools in the hands of the systems administrators and security professionals has helped, but we need to make them easier to use and manage.

Hale’s focus is on easier ways to work with these capabilities on a daily basis.

“Part of that is understanding what’s required, but another part is getting industry to help us in that by coming up with ideas that make some of these capabilities easier to implement and easier to operate,” Hale said.

“Wireless detection, I think, is one of the ones that falls exactly into that category, where we must make sure that we aren’t coming up with a solution that our soldiers, sailors and airmen aren’t going to be able to manage with day in, day out,” he added.

PROTECTING THE GLOBAL INFORMATION GRID

DISA’s goal is to protect and ensure the security of the GIG through information assurance. With continual collaboration with NSA, NIST and other partners, DISA has rapidly improved the security of the network. However, protection starts at the entry point to the GIG.

“You can’t build anything, you can’t protect the data, you can’t protect access, you can’t protect all of the other things we are trying to accomplish [without] a standard secure configuration,” said Orndorff. ★

BRAC RELOCATION OF DISA HEADQUARTERS TO FORT MEADE

DISA enjoyed a banner year with respect to the progress made in the huge effort to prepare for the relocation of DISA headquarters and the Joint Task Force-Global Network Operations (JTF-GNO) from Arlington, Va., to a new facility at Fort George G. Meade, Md.

Planning for the multiphased relocation, directed by the 2005 Base Realignment and Closure (BRAC) legislation, is ongoing. The initial movement phase, including the first large-scale relocation of organizations and personnel, will begin October 2010, and subsequent moves will be accomplished in several phases, concluding July 2011.

Following are a few highlights of the agency's accomplishments.

NEW DISA HEADQUARTERS CONTRACT AWARD AND DESIGN

The most tangible and visual aspect of the relocation is the construction of a 1.1 million square foot, multistory facility over a 35-month period to accommodate the 4,272 military, civilian and on-site contract-support personnel who will relocate to Fort Meade.

On February 29, 2008, the Army Corps of Engineers, Baltimore District, awarded the \$369.6 million contract to design and construct the new DISA headquarters at Fort Meade to Hensel-Phelps Construction Co. of Chantilly, Va.

A ground-breaking ceremony at the construction site was held on April 16, and more than 400 Maryland state and local business and community leaders attended, including congressional, state and local elected officials. Hensel-Phelps crews began actual ground preparation work in July 2008.

COMMUNITY RELATIONS

DISA continues its effort to reach out to and coordinate with new neighbors in Maryland, and the responses are always welcoming.

The DISA BRAC Transition Office orchestrated, on behalf of the DISA director, a visit to DISA and

JTF-GNO for the Maryland lieutenant governor and his BRAC sub-cabinet on October 12, 2007. The visit included reciprocal briefings by DISA/JTF-GNO and the Maryland officials and a tour of the JTF-GNO Global Network Operations Center.

On January 25, 2008, the DISA director hosted a visit to the agency for the executive members of the Fort Meade Regional Growth Management Committee (Maryland county executives and mayors). Participants included Ken Ulman, Howard County executive, and Kent Menser, director of BRAC actions for Howard County; John R. Leopold, Anne Arundel County executive, and his special assistant for BRAC, Bob Lieb; Jack B. Johnson, Prince George's County executive; Julia W. Gouge, president of the Board of County Commissioners for Carroll County, and Lawrence Twele, Carroll County economic director; Craig A. Moe, mayor of Laurel, Md.; Army Colonel Kenneth McCreedy, Fort Meade installation commander, and his executive officer, Bert Rice.

DISA BRAC Executive Dave Bullock met with U.S. Rep. John Sarbanes of Maryland on April 29. Bullock briefed the congressman about the DISA BRAC program with emphasis on transportation, commuting, education and other issues of concern to the DISA work force.

On June 9, Bullock provided an update to the Maryland Military Installation Council (MMIC) about the status of DISA BRAC projects. MMIC brings together the Maryland lieutenant governor, various cabinet secretaries, members of the Maryland congressional delegation, and local elected and business leaders to address issues that impact Maryland military installations.

AWARENESS AND OUTREACH PROGRAM

DISA's BRAC Transition Office facilitated numerous awareness and outreach events throughout the year.

On April 12, some DISA employees participated in the Greenlight Baltimore event, which was sponsored by "Live Baltimore" of the city's marketing department. Participating DISA employees received a free guided tour of Baltimore City and information on housing, transportation, education and numerous other family services in Baltimore.

On September 5, representatives from several Maryland state and county agencies set up

20 information booths at the 2008 DISA/JTF-GNO "End-of-Summer Picnic." They answered questions and provided information on housing, transportation, schools, businesses and recreation to more than 300 DISA employees.

Jack Penkoske, director of DISA's Manpower, Personnel, and Security Directorate, and Bullock have conducted several DISA/JTF-GNO town hall meetings to provide a forum for employees to receive first-hand information on BRAC updates and answers to their BRAC-related questions. The first town hall meeting was held on July 15 at the main headquarters building, and subsequent meetings took place at two other DISA headquarters sites. On each occasion, more than 100 DISA employees attended. The meetings were also broadcasted live via one of the agency's electronic collaboration tools.

The BRAC Transition Office sponsored an employee-orientation field trip to Fort Meade on November 6. This was the latest in a continuing series of periodic orientation trips. The Fort Meade installation commander, the Fort Meade morale, welfare, and recreation director, and the DISA BRAC executive gave informative briefings to the DISA employees. After the presentations, the employees were provided a narrated tour of Fort Meade, including the DISA headquarters building site.

RESOURCE MANAGEMENT

The BRAC Transition Office developed a funding strategy for building and occupying a new DISA facility at Fort Meade that satisfies all identified requirements within available funds. Starting with a \$70 million shortfall, the BRAC Office worked aggressively with the Army Corps of Engineers and our supporting architecture and engineering personnel to find opportunities for savings that preserved the project scope.

During fiscal year 2008, the DISA BRAC Transition Office successfully negotiated with the Department of the Army BRAC Office to



secure funding to support human resources benefits for DISA employees at Fort Monmouth, N.J., who are impacted by the BRAC closure of that installation.

Also, the DISA BRAC Transition Office successfully prevailed upon the Air Force BRAC Office to provide \$1.5 million to relocate public key infrastructure (PKI) processing and provide human resources benefits for DISA employees impacted by the closure of Buckley Annex in Denver, Colo.

RECOGNITION FOR THE DISA BRAC TRANSITION OFFICE

On April 10, 2008, the BRAC Transition Office received the DISA Outstanding Non-Technical Program/Project of the Year award. Selection was based on demonstrated initiatives involving the development and implementation of new ideas, processes, plans and strategies that improved the quality of services provided by DISA organizations.

Although much has been accomplished, the work and the pace of planning, coordinating, and implementing this incredibly complex move will rage on unabated through 2011. ★

An aerial view of the construction site of DISA's new 1.1 million-square-foot facility at Fort George G. Meade, MD. A ceremonial ground-breaking ceremony was held on April 16.

Welcome to the Evolution.



The Sectera® vPer™ Universal Secure Phone is the next step in end-to-end high assurance security for voice communications. The vPer Phone is a single desktop solution for:

- Both non-secure and secure (Top Secret and Below)
- PSTN connectivity
- Voice over IP connectivity
- Cost-effective migration from PSTN to VoIP
- STE interoperability

The Universal Secure Phone

Protect your investment and evolve into the next generation of technology. The versatile Sectera vPer Phone provides the flexibility for multiple networks. All other solutions seem...well, primitive.

781-455-2800/888-897-3148 • secure.communications@gdc4s.com • www.gdc4s.com/vPer

General Dynamics Secure Communications: We Bring You What's Next



GENERAL DYNAMICS
C4 Systems

See the live demonstrations at the 2009 Unified Information Assurance User Conference and Training event May 27-28, 2009 in Las Vegas. www.gdc4s.com/userconference



MOBILE MEDICAL™

ARRIVE PREPARED. PACK TO SAVE LIVES.

HARDIGG MILITARY MEDICAL CASES SPECIALIZE
IN FAST-ACCESS, LIGHTWEIGHT PROTECTION.

Watertight, airtight and impact resistant – Hardigg Cases are engineered and designed in tandem with military medical professionals. No other cases transport sensitive diagnostic gear and lifesaving equipment into the field with this level of confidence. From wide X-ray pockets and compartmentalized drawers to decontaminable and fire-resistant models – Mobile Medical cases are customizable to ensure immediate, reliable access anywhere. Visit our website for the full product listing and more Hardigg military solutions.

147 North Main Street, South Deerfield, MA 01373 • 800.542.7344 • MilitaryCases.com
Hardigg.com. For more information, visit our website or contact our GSA specialist at Military@Hardigg.com or 413-665-2163. Contracts #GS-15F-0019M, GS-07F-9216S. Hardigg accepts Government IMPAC cards and Government Visa cards. Trademarks owned by Hardigg Industries, Inc. ©Hardigg Industries, Inc. 2007



MOBILE MEDICAL.

GSA CONTRACTS GS-15F-0019M
GS-07F-9216S
800.542.7344 • MilitaryCases.com
Hardigg.com

BATTLE PROVEN

