

March 2003

# *intercom*

*Journal of the Air Force  
C4 Community*



**SPOTLIGHT ON  
DEFENSE AGENCIES**

**Air Force Chief of Staff**

Gen. John P. Jumper

**Deputy Chief of Staff for  
Warfighting Integration**

Lt. Gen. Leslie F. Kenne

**Deputy Chief of Staff for  
Air and Space Operations**

Lt. Gen. Ronald E. Keys

**Deputy Chief of Staff for  
Installations and Logistics**

Lt. Gen. Michael E. Zettler

**Director of CAISR Infostructure  
DCS for Warfighting Integration**

Maj. Gen. Charles E. Croom Jr.

**Commander,  
Air Force**

**Communications Agency**

Col. David J. Kovach

## Editorial Staff

**AFCA Chief of Public Affairs**

Lori Manske

**Executive Editor**

Len Barry

**Editor**

Tech. Sgt. Michael C. Leonard

This funded Air Force magazine is an authorized publication for members of the U.S. military services.

Contents of the *intercom* are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or the Department of the Air Force.

Editorial content is edited, prepared and provided by the public affairs office of the Air Force Communications Agency.

All photos are U.S. Air Force photos unless otherwise specified. Photo submissions are encouraged in the form of high-resolution digital images or 35 mm prints.

News copy, photos, story ideas and comments may be e-mailed to [intercom@scott.af.mil](mailto:intercom@scott.af.mil), or mailed to AFCA/PA, *intercom*, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222. Fax is DSN 779-6129 or (618) 229-6129. Editorial staff may be contacted at DSN 779-5690, or (618) 229-5690.

*intercom* can be found on the World Wide Web at <http://public.afca.scott.af.mil/intercom.htm>



### 'X marks the spot'

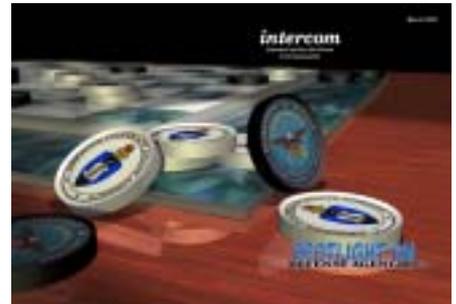
Frequency spectrum access ... job one for Air Force Frequency Management Agency	Page 4
New vector for AF Agency for Modeling and Simulation	Page 5

### Spotlight on Defense Agencies

Defense Advanced Research Projects Agency	Page 6
Defense Contract Audit Agency	Page 7
Defense Commissary Agency	Page 8
Defense Contract Management Agency	Page 10
Defense Intelligence Agency	Page 12
Defense Finance and Accounting Service	Page 13
Defense Information Systems Agency	Page 14
Defense Security Cooperation Agency	Page 17



### On the cover



Cover design by  
Staff Sgt. Kevin Williams, AFCA



Visit the Computer Based  
Training System Web site at  
<http://usaf.smartforce.com>

Defense Legal Services Agency	Page 17
Defense Logistics Agency	Page 18
Defense Security Service	Page 20
Defense Threat Reduction Agency	Page 21
Missile Defense Agency	Page 26
National Imagery and Mapping Agency	Page 27
National Security Agency	Page 28
Pentagon Force Protection Agency	Page 28

### *in other news*

<i>Lt. Gen. Winston Powers</i>	
Former DCA director passed away Feb. 6	Page 29
Comm and info personnel high on request list	Page 32
32nd AOG deploys to support GWOT	Page 36
DOD program helps develop civilian leaders	Page 38



## Frequency spectrum access ... job one for AF Frequency Management Agency

**By Col. Steve Woolf**

*AF Frequency Management Agency commander  
Pentagon*

You can neither see it nor touch it but it's a critical thread throughout our Air Force's kill chain. What could be so invisible yet so vital to our national security? It's the radio frequency spectrum. Gaining access for the warfighter to this finite, highly regulated, and coveted national resource is the prime mission of the Air Force Frequency Management Agency.

AFFMA may be small in size with only 36 authorizations but is big in responsibility and capability. We are responsible for acquiring RF spectrum access for the Air Force whether in our homeland, in other nations, or in space.

Our responsibility starts in the conceptual phase of system development by advising which part of the spectrum is best for a certain capability and requesting a "building permit", or certification, from the President's spectrum manager, the National Telecommunications and Information Administration. This "building permit" gives the Air Force the authorization to develop a capability in a particular portion, or band, of the RF spectrum best suited for the desired effect and in accordance with national and international guidelines. AFFMA also works closely with spectrum managers in the combatant commands to obtain similar authorizations in foreign nations. When it comes to space, AFFMA works with NTIA and the Federal Communications Commission to register U.S. satellites with the International Telecommunications Union, or ITU, for operation in particular orbits and on particular frequencies.

When a capability is ready for use, a "license" to radiate, known as a frequency assignment, is required. AFFMA experts obtain this "license" from NTIA which gives the AF the right to transmit on a specific frequency within the U.S. and its possessions while providing legal protection from un-

authorized users. Combat command spectrum managers request similar frequency assignment approvals from desired nations within their area of operation. In space, this "license" to operate is acquired via the registration process mentioned above involving the ITU.

It is surprising to note that the entire federal government has exclusive rights to only 7 percent of the RF spectrum below 30 GHz. The civil sector has exclusive rights to 30 percent and the remaining 63 percent is shared. As requirements grow and supply is limited, the value of spectrum greatly increases in today's economy. The Congressional Budget Office estimates the auction value of 1 MHz of spectrum at around \$100 million each. Given the importance of spectrum to federal and civil entities, the Air Force continually strives to be a good spectrum neighbor and participates at all levels to ensure a proper balance between national security and national economy.

One of AFFMA's important functions is to represent the Air Force on numerous national committees along with other federal agencies and work closely with the FCC to ensure the right balance of spectrum use is achieved. A recent example involved the DOD agreeing to vacate the majority of a 45 MHz portion of spectrum to allow commercial development while preserving critical Air Force capabilities involving precision guided munitions, satellite uplinks, air combat training, and flight test telemetry.

Modern weapon systems cannot operate without access to the RF spectrum. Spectrum access is the enabler that allows split second, machine-to-machine interfaces in order to achieve the desired combat effect. As we continue to refine our spectrum access, the kill chain is tightened and our effects-based capabilities can be measured in fractions of seconds thanks to the outstanding spectrum experts in the AFFMA.

# *New vector for AF Agency for Modeling and Simulation*

**By Col. Grant F. Herring**

*Commander, AFAMS  
Orlando, Fla.*

The Air Force Agency for Modeling and Simulation was spotlighted in the June 2002 *intercom* with an article explaining our role and mission within the Air Force deputy chief of staff for Warfighting Integration, or AF/XI. As the field operating agency responsible for AF-level modeling and simulation, or M&S, policy implementation, integration and support, AFAMS provides unrestricted opportunities to explore and achieve full spectrum dominance.

AFAMS' responsibilities include M&S integration and coordination; decision support and consultation; concept evolution and communication; planning and status monitoring; top-level policy implementation; and top-level program management. Although our major thrust as the top-level M&S support agency has not changed, some of the programs supported have changed. This update will provide information about AFAMS' new vector.

As a member of the AF/XI team, AFAMS has a direct impact on many Air Force M&S efforts. Some of the efforts include:

**Policy and decision support** - AFAMS is nearing publication of the Air Force Modeling and Simulation Strategic Plan. This all-encompassing document is a high-level plan that will outline the AF M&S mission, vision, strategic goals, objectives, measures and offices of primary responsibility. Other policy support initiatives include concept of operations development for programs including Joint Synthetic Battlespace and Distributed Mission Operations, both major contributors to AF training transformation. Additionally, AFAMS provides links to key Air Force and DOD modeling and simulation players. The Theater Battle Arena, an operating location of AFAMS located in the Pentagon, has a direct impact on linking the Pentagon to major Air Force and DOD exercises and experiments as well as decision support tools for

the warfighter.

**M&S integration** - AFAMS has established and continues to lead efforts assuring M&S standards are established and enforced while integrating legacy and newly developed simulators and simulations. Additionally, the leadership AFAMS provides in the M&S architecture arena will assure new programs are capable of interoperable functionality. Data standards also receive a great deal of attention with reuse driving the anticipated future cost of data base generation to significantly lower levels.

**M&S innovation** - The importance of M&S spans many areas, but science and technology is one of the major thrusts of AFAMS. Our efforts to assure the inclusion of the latest technology in M&S initiatives are vitally important to the warfighter. AFAMS is working closely with AFRL, AFMC, AF Battle Labs, Joint forces, and industry to assure M&S stays abreast of the latest science and technology.

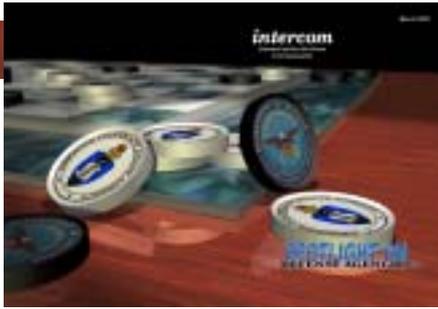
**M&S representation of air and space power** - Simulations have traditionally been criticized for their inaccurate replication of air and space power activities. Working with developers of both new and legacy systems, AFAMS is assuring that future simulations and upgrades to legacy simulations adhere to latest doctrine and accurately portray the power air and space bring to the warfighter.

**M&S Professional Development and Readiness Support** - AFAMS is establishing a computer based training capability for M&S professionals that will significantly improve productivity for newly assigned personnel. Top-level support to major AF and DOD exercises and experimentation will continue to be a major portion of the AFAMS mission as we continue to mature the fighting force using the latest decision support tools enabled by M&S.

**Joint, interoperable, and reusable M&S** - AFAMS leverages many existing programs to

See **AFAMS** Page 7





## *Defense Advanced Research Projects Agency*

*Pursuing high risk, high pay off*

The Defense Advanced Research Projects Agency, Arlington, Va., is the central research and development organization for the Department of Defense. It manages and directs selected basic and applied R&D projects, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions.

DARPA's mission is to develop imaginative, innovative and often high-risk research ideas offering a significant technological impact well beyond the normal evolutionary developmental approaches; and to pursue these ideas from the demonstration of technical feasibility through the development of prototype systems.

The **Advanced Technology Office** researches, demonstrates and develops high payoff projects in maritime, communications, special operations, command and control, information assurance and survivability mission areas. ATO adapts advanced technologies into military systems and exploits emerging technologies for future programs.

The **Defense Sciences Office** pursues the most promising discoveries and innovations in science and engineering to create paradigm shifts in defense capabilities. DSO emphasizes programs in medical approaches to biological warfare defense, biology, materials and advanced mathematics.

The **Information Awareness Office** develops and demonstrates information technologies and systems to counter asymmetric threats by achieving total information awareness useful for preemption, national security warning and national security decision-making.

The **Information Processing Technology Office** focuses on inventing the networking, computing, and software technologies vital to ensuring DOD military superiority.

The **Information Exploitation Office** develops sensor and information system technology and systems with application to battlespace awareness, targeting, command and control, and the supporting infrastructure required to address land-based

threats in a dynamic, closed-loop process. IXO leverages ongoing DARPA efforts in sensors, sensor exploitation, information management, and command and control.

The **Microsystems Technology Office** focuses on heterogeneous microchip-scale integration of electronics, photonics and microelectro-mechanical systems. Their high risk/high payoff technology is aimed at solving national level problems of protection from biological, chemical and information attack and to provide operational dominance for mobile distributed command and control, combined manned/unmanned warfare, and dynamic, adaptive military planning and execution.

The **Special Projects Office** develops systems solutions, along with enabling technologies, to counter current and emerging threats. In the area of current challenges, SPO focuses on affordable, precision kill of movers, emitters, and concealed (including underground) targets. In the area of emerging threats, SPO focuses on active defenses against biological weapons, proliferated, low-cost/low-technology air vehicles and missiles, and against GPS jamming.

The **Tactical Technology Office** engages in high-risk, high-payoff military research, emphasizing "system" and "subsystem" approach to development of aeronautic, space and land systems and embedded processors and control systems.

### **DARPA Support Offices**

The **Office of the Comptroller** prepares and submits the consolidated annual agency budget, and manages the planning, programming and budgeting system process.

The **Contracts Management Office** plans, negotiates and awards contracts, grants and agreements for select new-start technology projects and for consortium and other cooperative projects.

The **Office of Management Operations** provides administrative support to the director, technical office directors, program managers, and DARPA staff. (*DARPA Web site*)

# Defense Contract Audit Agency

## THE audit organization supporting the warfighter

**By Stan Arnold**

*Program Manager, Technical  
Audit Services  
Defense Contract Audit Agency*

The Defense Contract Audit Agency, or DCAA, under the authority, direction and control of the under secretary of defense (Comptroller), is responsible for performing all contract audits for the Department of Defense, and providing accounting and financial advisory services regarding contracts and subcontracts to all DOD components responsible for procurement and contract administration. DCAA was established in 1965 for the purpose of reducing duplication by consolidating contract audit activities of the military services. Since then, it has emerged as the best value provider of contract auditing and financial advisory services to components within the DOD as well as to non-DOD government agencies.

### **Vision and Accomplishments**

DCAA's vision states in part: "Our aim is to be **THE** audit organization with the foremost reputation for competence, integrity, and customer satisfaction..." Our contribution to the warfighter continues to be our ability to save contract funds that can be used or redirected to other requirements. These savings result from DCAA's efforts to audit and monitor DOD acquisitions of equipment, materials and/or services from contractors and universities. Based on our audit results, DCAA has re-

turned \$2.4, \$3.2, and \$2.5 billion in each of the last three fiscal years. These savings result in substantial returns on investment; for example, the return on investment for these fiscal years (savings vs. agency budget) ranged from \$6.30 to \$8.40 for every budgeted dollar.

DCAA continues our goal to be THE audit organization, even during the current difficult times when we must all sacrifice budget and staffing to support the warfighters. To continue our dedication to customer service, we have created innovative services for our customers that make the most of our staff resources. Additionally, we continue to improve our information technology capability with both DCAA and DOD automated systems, which allows us to provide better services more expeditiously.

### **Customer Liaison Services**

DCAA supports the acquisition reform process by augmenting the field audit staff with auditors dedicated to customer liaison services – the **financial liaison advisor**, or **FLA**. DCAA created the FLA function by combining two existing, customer-oriented services, the **procurement liaison auditor**, or **PLA**, and the **financial advisor**, **FA**. The new FLA function incorporates the benefits of the PLA and FA services into one position dedicated to customer liaison services.

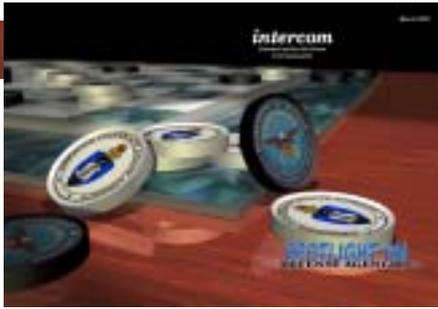
See DCAA Page 11

**AFAMS**

*From Page 5*

assure the warfighter gets the maximum benefit from limited M&S investments. Major efforts in this area include the Air Force Modeling and Simulation Training Toolkit and the Air Force Modeling and Simulation Resource Repository. The AFMSTT has taken legacy, off-the-shelf simulations, and a few new programs, to create a highly effective air and space simulation for training Joint and AF personnel in the Air Operations Center. This program has been exceptionally effective and is delivering quality training at lower cost than a new development. The AFMSRR, a knowledge management tool, is an invaluable virtual card-catalog of architectures, models, simulators, simulations, data bases, papers, studies, and more – all with the intent of providing a vehicle to discover resources for reuse and avoid duplicating efforts at considerable savings to the AF M&S community.

AFAMS has a full set of responsibilities important to AF goals for warfighter integration and training transformation. In addition, new efforts are being made to address homeland security by incorporating M&S capabilities. As we continue to advance our M&S initiatives and concepts to train, mission rehearse, and provide decision support to operations, we take pride in knowing the power that M&S brings to the warfighter will have a major impact on the outcome of future hostilities.



## *Defense Commissary Agency*

Delivering the benefit through technology

**By Florence Dunn**  
*DECA*

The Defense Commissary Agency, headquartered at Fort Lee, Va., manages and operates 276 commissaries worldwide through four regional offices in Virginia Beach, Va., San Antonio, McClellan, Calif., and Kapaun AS, Germany.

Air Force Maj. Gen. Michael P. Wiedemer, DeCA director, reports to the undersecretary of defense for personnel and readiness through the assistant secretary of defense (force management policy), and subject to the operational supervision of the Commissary Operating Board.

DeCA is managed in a cost-and-output culture through four business areas: operations, product support, resources, and capital investment. Activity-based management is a way of life at DeCA, enabling the agency to provide greater savings for service members and families on the goods and services they buy than at any other time in history.

Commissaries sell foodstuffs and household supplies to members of the military services, retirees and their families and other authorized shoppers, providing a "taste of home" no matter where they are stationed, at an average savings of 30 percent or more when compared with commercial

prices. These savings are worth more than \$2,400 a year for a family of four. Commissary shoppers purchase items at cost plus a 5 percent surcharge, which covers the construction of new commissaries and the modernization of existing ones.

The agency depends heavily on automation to carry out its mission of providing an efficient and effective worldwide system of commissaries for the resale of groceries and household supplies at the lowest practical price while maintaining high standards for quality, facilities, products and services.

The agency's more than 17,900 civilian employees and military members are dedicated to enhancing customers' shopping experience. To achieve this, DeCA is implementing several information technology initiatives, designed primarily to improve customer service while also addressing the efficiency of personnel and systems.

Each of DeCA's IT initiatives must produce the twin benefits of greater savings and service, and lower operating costs.

Computer Assisted Ordering, or CAO, captures front-end data and determines the proper number of items to be reordered. Using CAO, commissary workers can proactively manage product availability and maintain an effective stock level – putting the right product on the shelf at the time customers want to buy it.

Electronic shelf labels, or ESLs, a high-tech alternative to the paper labels used by most supermarkets and other mass retail stores to indicate product pricing, have been implemented in some commissaries. ESL tags clearly display product information including accurate pricing. The information displayed on the ESL is the same information used by the checkout system, ensuring no price discrepancy between the shelf tag and the cash register.

DeCA, like most government agencies and supermarket chains, is working hard to reduce costs and maximize productivity through strategic investments in information technology.



*DeCA photo by Dr. Pete Skirbunt*  
**Chief Master Sgt. Cynthia McNeas shops at the Dover AFB, Del., commissary.**

The Commissary Operations Management System, COMS, is just one technology DeCA uses to improve internal management processes. COMS provides managers with real-time access to operational data, such as sales, savings, promotions and customer demographics – information in the data warehouse that they can use in making decisions aimed at increasing sales and providing greater savings.

Information on costs and sales permits timely spotting of savings and revenue trends allowing sufficient time to take corrective measures or to benefit from the trend. The data warehouse also allows the agency to cut overhead costs by providing managers with an instant view of key data on costs, sales and inventory without filtering through several organizational layers.

DeCA has saved considerable operating expenses by consolidating and automating business processes, such as ordering and vendor bill paying, while also moving the agency toward more modern platforms and data management strategy.

A technology tool aimed at customer service is DeCA's Web site, [www.commissaries.com](http://www.commissaries.com). Shoppers can find store locations, hours, promotions, recipes and a customer feedback option to reach DeCA electronically. Each commissary has its own Web page with promotions and sales information.

Employee communication is another crucial element in improving customer service. General Wiedemer has increased direct personal communication with employees by soliciting their input and ideas via the agency's intranet. He has received from employees hundreds of ideas to improve the way DeCA operates, many of which have already been implemented throughout the agency from top to bottom, saving thousands of hours of effort.

DeCA's trading partners -- its distributors and suppliers -- are another important and invaluable component of the agency's ability to successfully deliver the commissary benefit.

The agency's award-winning electronic commerce program improves business-to-business exchange of information by applying industry-standard electronic data interchange transactions.

The agency is completing deployment of leading-edge encryption technology and is partnering with industry to develop new information protection solutions. These ensure that data is secure, and, more importantly, that customers' personal data is not compromised.



*DeCA photo by Dr. Pete Skirbunt*  
**Sue Mills, store worker, gathers inventory data at the Dover AFB commissary using a portable data entry device.**

As for the future, suppliers of IT products are improving their technology day-by-day. With this in mind, DeCA has a formal process to determine which of the many technology products available will best suit its business requirements.

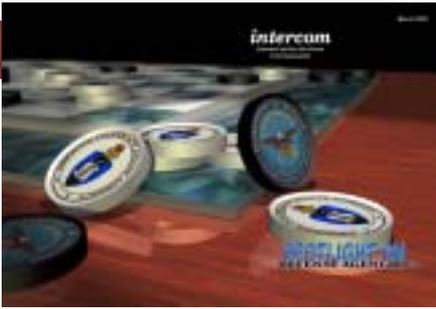
Self-checkout stations that will allow customers the option to scan their own groceries are being considered.

As DeCA increases the content and capabilities of its data warehouse, store managers and employees will have real-time access to decision-making information for merchandising, ordering, promotions and product selections on their desktop computers. Data warehouse expansion reduces some reporting requirements and allows workers to spend more time on the commissary floor interacting with customers.

DeCA has taken initial steps to acquire a new, commercial point-of-sale system that will provide better inventory management, faster and more accurate customer checkouts and more rapid and secure transaction processing for debit and credit cards.

Actions are under way to reduce hardware and software maintenance costs by consolidating the processing centers, consolidating servers and eliminating legacy systems as the agency moves to the DOD standard architecture. By modernizing technology infrastructure, the equipment and human effort required in producing more decision support information will be reduced.

The Defense Commissary Agency will continue to focus its information technology efforts on delivering first-class facilities, products and services, effectively and efficiently, to its deserving customers.



## *Defense Contract Management Agency*

### DOD's 'eyes and ears' in factories

As a DOD combat support agency, the Defense Contract Management Agency, or DCMA, provides customer-focused acquisition support and contract management services to ensure warfighter readiness, 24/7, worldwide. DCMA's 11,000 acquisition professionals are DOD's "eyes and ears" in the factories. They assure industry's products meet performance requirements and are delivered on time and at the agreed-to costs. Headquartered in Alexandria, Va., with 65 major field locations with more than 900 operating sites, DCMA oversees 320,000 contracts worth more than \$860 billion. The Agency strives to be an indispensable partner, providing military and civilian customers flexible and responsive acquisition life-cycle solutions.

#### **DCMA IT Initiatives**

DCMA professionals serve as "information brokers" and in-plant representatives for military, federal, and allied government buying agencies — both during the initial stages of the acquisition cycle and throughout the life of the resulting contracts. Before contract award, DCMA provides advice and services to help construct effective solicitations, identify potential risks, select the most capable contractors, and write contracts that meet the needs of customers in DOD, federal and allied government agencies. After contract award, DCMA monitors contractors' performance and management systems to ensure that cost, product performance, and delivery schedules comply with the terms and conditions of the contracts.

DCMA is a recognized leader of, and contributor to, many of DOD's business reform initiatives. Those initiatives' goals are to improve the nation's defense in the most economical and efficient ways possible. For example, DCMA is a member of the Acquisition Governance Board for the DOD Financial Management Enterprise Architecture. DCMA was also previously the co-chair of the DOD Paperless Contracting Integrated Product Team. DCMA is the co-chair of the Joint Requirements

Board for Wide Area Work Flow Receipt and Acceptance, or WAWF-RA. This Internet based program allows DOD vendors to submit and track their invoices and receipt/acceptance documents electronically. WAWF-RA allows vendors to be paid faster and reduces interest payments made by the government. For example DCMA has achieved 99.98 percent on-time payments for its contracts and has only paid \$54.86 in interest this year.

In addition to external DOD's business reform initiatives, DCMA has been transforming its own IT infrastructure and applications. One such initiative has been the establishment and continual fine-tuning of a DISA-approved Community of Interest Network, or COIN. DCMA's COIN has allowed it to significantly increase communications bandwidth across major DCMA locations while reducing overall costs. It has made possible the consolidation of IT resources such as servers, as well as providing affordable capacity for DCMA's video teleconference centers.

DCMA is also taking advantage of the latest technology to efficiently develop and field new Web based software applications. Client/server applications that originally took years to develop and deploy are now being built and fielded in months. DCMA has eight Web-based applications operational and 10 applications in development and testing.

DCMA is also working to provide more access to our applications and data to our customers. This will allow our customers to query DCMA databases for their use. For example at the DCMA Web site at <http://home.dcma.mil/dcma-pi/nsnlookup.htm> customers can query current DCMA contract data by national stock number or part number to see all DCMA-administered contracts, where that item is on order, and can also see all those contracts' delivery schedules. That information is useful to customers when they need to identify quick-response alternative sources of supply.

**DCAA**  
From Page 7

The FLA will become DCAA's primary point of contact to the procurement and contract administration activities. In many cases, the FLA also functions as the activity's representative and primary point of contact with DCAA. As such, the FLA provides a wide spectrum of services ranging from expediting advisory audit reports to communicating complex positions in the resolution of sensitive audit issues.

The FLA also provides on-site financial advice to contracting officers at major acquisition offices. The FLA assists them in implementation of acquisition reform goals and in the negotiation of fair and reasonable contract prices. Acquisition reform goals include reducing cycle-time and streamlining contracting processes by emphasizing contracting officer flexibility to make fair and reasonable price determinations using the most expedient evaluation methods. The FLA provides the acquisition officials with on-site information and assistance when there is neither time nor practical need to request information from DCAA field audit offices.

**Information Technology Initiatives**

DCAA has fully embraced the Presidential, federal government, and DOD initiatives for the paperless environment and electronic business. DCAA has integrated these initiatives into our strategic plan and has actively pursued their implementation. Our strategic plan initiatives include:

**Electronic Invoicing.** DCAA is active in the DOD initiatives for paperless contract financing. DCAA has responsibilities for approving some contractor requests for payment and has processed some of these requests through existing electronic payment systems. DCAA is participating in the enhancement of the **Wide Area Workflow** system that will dramatically enhance the electronic approval process for contractors' public vouchers.

**Information Security.** In accordance with DOD requirements, DCAA is quickly implementing the information assurance components to protect information systems. The Agency is issuing Common Access Cards to all personnel and is employing Public Key Infrastructure technology to restrict access to electronic data. DCAA will protect electronic transmittal of audit-related documents using PKI to sign and encrypt the electronic communication.

**Electronic Submissions.** DCAA set a goal to increase the number of electronic submissions from contractors. These submissions include pricing proposals and incurred cost submissions. Electronic submissions allow the audit staff to quickly and seamlessly integrate data into DCAA software, which reduces response time on audit services.

**Enhanced Audit Software.** DCAA continues to improve the audit software that was developed to meet the paperless initiatives. The **Audit Planning & Performance System** software provides the audit staff with the tools to create and store electronic working papers and audit reports.

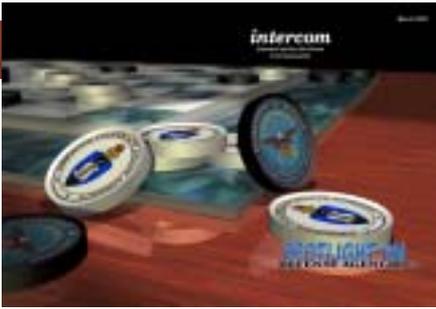
**Electronic Archiving and Storage.** DCAA is implementing an electronic archiving and storage system. The system will provide greater security over documents as well as reduce the cost of storage when compared to paper storage.

DCAA will continue to enthusiastically pursue the paperless and electronic business initiatives. We recognize that these initiatives benefit not only our Agency, but more importantly they benefit our customers and the warfighter. If we are successful, we can accomplish our goal to be:

***THE audit organization with the foremost reputation for competence, integrity, and customer satisfaction....***

For more information about the Defense Contract Audit Agency, please visit our public Web site at [www.dcaa.mil](http://www.dcaa.mil).





## *Defense Intelligence Agency*

Crossing all aspects of military intel

The Defense Intelligence Agency is a Department of Defense combat support agency and an important member of the U.S. intelligence community. With more than 7,000 military and civilian employees worldwide, DIA is a major producer and manager of foreign military intelligence. It provides military intelligence to warfighters, defense policy-makers and force planners, in the DOD and the intelligence community, in support of U.S. military planning and operations and weapon systems acquisition.

The director of DIA is a three-star military officer who serves as principal advisor to the Secretary of Defense and to the chairman of the Joint Chiefs of Staff on matters of military intelligence. The director also chairs the Military Intelligence Board, which coordinates activities of the defense intelligence community.

DIA is headquartered at the Pentagon in Washington, D.C., with major operational activities at the Defense Intelligence Analysis Center, Washington, D.C., the Armed Forces Medical Intelligence Center, Frederick, Md., and the Missile and Space Intelligence Center, Huntsville, Ala.

Its workforce is as diverse as its missions. Its workforce is skilled in the areas of military history and doctrine, economics, physics, chemistry, world history, political science, bio-sciences, and computer sciences, to name a few.

They respond to the needs of customers from the President of the United States to the soldier in

the field. They cover all aspects of military intelligence requirements – from highly complex missile trajectory data to biographical information on foreign military leaders.

One of its directorates is the **directorate for Information Systems and Services**. It is the primary intelligence information services support center for the DIA. It provides customer support and oversight of information technology acquisition across the defense intelligence enterprise.

Using the latest information technologies, this directorate monitors, maintains and supports DIA network operations around the world with 24-hour-a-day, 7-day support. It carries out the management and accreditation of DOD Intelligence Information Systems.

The directorate manages and

maintains one of the world's most robust communications systems, the Joint Worldwide Intelligence Communications System. JWICS is a secure, high-bandwidth system providing full motion video teleconferencing and data exchange among major intelligence nodes. It also engineers and integrates technologic initiatives such as the Joint Intelligence Virtual Architecture. JIVA is a virtual workstation permitting interoperable and integrated intelligence analysis through advanced computer systems and modern database applications that enable analysts to work collaboratively regardless of where they are based or deployed in the world.

*(DIA Web site)*



# Defense Finance and Accounting Service

## Collaboration and integration through the DFAS system life cycle

By Elliott Chikofsky

*Defense Finance and Accounting Service*

The Defense Finance and Accounting Service provides and manages the back office operations to ensure the warfighter and support operations are paid, equipped and supplied.

DFAS is the world's largest finance and accounting operation. In fiscal year 2002, the agency disbursed more than \$346.6 billion, paid 5.7 million people, made 7.3 million travel payments and performed more than 124 million accounting transactions while saving the DOD more than \$144 million. With this scale of operation, efficiency in delivering services is critically important. DFAS' success allows DOD to spend less than one half of one percent of its budget on our finance and accounting services.

Information technology is the principal tool in delivering efficient systems to meet our financial support mission. IT in DFAS is a continuous challenge of integration, evolution and innovation.

### **DFAS System Life Cycle**

Planning and communication are two factors that are central to success in developing and maintaining world-class information systems. A key mechanism to ensure adequate planning and communication in our IT management process is the DFAS System Life Cycle, or SLC.

Life cycle management techniques recognize the stages of a development process, the activities that occur at each stage, and the information that must be created or collected to verify work completion or provide input to later stages. Traditionally, the life cycle process has been viewed as management-by-document, which has earned it an undesirable reputation. But, a life cycle approach can be a unifying framework, instead of a burden. Within DFAS, we are recognizing how our SLC can give program managers context and direction for improved planning and sound implementation.

First and foremost, the DFAS SLC emphasizes active customer participation at all stages of IT development. We team with customers to understand requirements, establish test and acceptance criteria, and resolve system problems. This cooperative process encourages flexible, evolutionary development and innovative solutions.

The SLC framework encourages realistic plan-

ning and an implementation process that has sound management accountability. It gives us visibility into cost, schedule, requirements, and technical plans and progress. This allows each program manager to assess risk and to monitor and report the program's status and issues effectively. It also allows meaningful executive oversight across the many programs throughout the agency.

### **Integrated Framework**

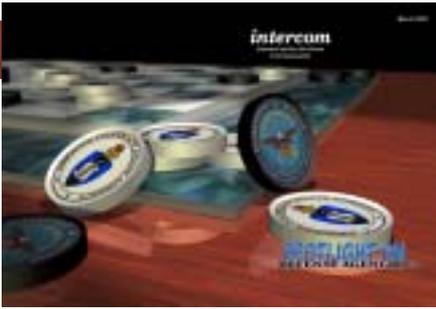
The DFAS SLC serves as a single, actionable framework that integrates the many diverse requirements that program managers must meet. For example, information assurance and security are critical concerns for DFAS and our customers. Our systems must follow the DOD IT Security Certification and Accreditation Process, or DITSCAP. While such an initiative is a stand-alone process in many agencies, DFAS incorporates it directly into the SLC framework. DITSCAP activities are included as tasks in each program's life cycle checklist. As such, information assurance certification becomes a natural part of the system development activity, rather than being an add-on or an afterthought. Similarly, configuration management, quality assurance, and customer assessment are interwoven with the rest of the SLC activities.

The DFAS SLC also saves time and effort in complying with the ever-changing procedural environment in which we develop systems. We keep the SLC up-to-date as the primary source of guidance. If a program is following the DFAS SLC, that program is implicitly, and traceably, following current regulatory guidance. This allows program managers to concentrate on the quality of their systems and meeting customer needs.

### **SLC in Professional Growth**

The DFAS SLC also has a role in promoting knowledge and professional growth for our people involved in systems development and management. Our SLC Web site presents the life cycle activities and tasks from a variety of views and perspectives. This contributes to job understanding and increasing job skills. Through all this, it becomes clear how the DFAS SLC weaves many different task threads throughout the organization.

The DFAS SLC can be found on our DFAS.MIL Web site under the Reference Library in the Process Asset Library. It is available on our public Web site.



## *Defense Information Systems Agency*

### **Attaining interoperability through net-centricity**

**By Frank M. Holderness**  
*DISA*

The Department of Defense is undergoing an Information Age transformation that embraces a Network-Centric Warfare, or NCW, concept. Relatively new, NCW capitalizes on innovative technologies to provide the warfighter with capabilities to accomplish missions efficiently and effectively. Once fully implemented, these capabilities will have global implications, extending across the entire spectrum of military operations worldwide.

Before NCW can be implemented organizationally across DOD, there must be a strategic focus on interoperability. Interoperability allows diverse systems to work together effectively. If ignored, systems are unable to share information, presenting a 'roadblock' on the information highway. However, when given the proper roadmap, one can plot out the course necessary to overcome each roadblock as encountered.

DISA, a combat support agency under the direction of the Office of the Assistant Secretary for Defense for Command, Control, Communications, and Intelligence, established the IN directorate in October 2001 to ensure that end-to-end system capabilities would continue to evolve in accordance with the tenets of NCW. IN also ensures end-to-end interoperability of all Global Information Grid, or GIG, systems, and provides life-cycle test, evaluation, certification and technical support for national security and information technology systems comprising the GIG.

#### **The Role of Standards**

An additional objective of IN is to ensure all GIG systems and capabilities are compliant with the appropriate policy, regulations, guidance and standards. Standards are key to information exchange and attaining interoperability. IN's Joint Interoperability Test Command, or JITC, certifies all DOD systems and capabilities operationally adhere to those interoperability requirements and

standards. This is fundamental to the concept of NCW. Specific measures must be taken to gauge the progress being made towards attaining interoperability for a net-centric based force.

IN also represents DOD within organizations producing standards, ensuring that the department's vested interests are taken into consideration whenever an IT standard is being promulgated. Along with that, IN ensured that the right standards are being developed. If using too many standards, or too few, the repercussions felt across the DOD could be disastrous. To counter such drawbacks, numerous measures have been put in place in the form of analysis and review cycles, technical forums and subject matter expert working groups and committees.

There are several ongoing standards-based initiatives within IN that proliferate both information superiority and interoperability on behalf of the warfighter. Efforts such as the DOD Technical Reference Model, Joint Technical Architecture, and Global Information Grid Architectural serve as the foundation for several of DISA and DOD's pillar programs, including Net-Centric Enterprise Services and the Defense Information System Network.

One of the provisions under the NCW concept is to develop International Net-Centricity-capabilities that can be effectively employed during allied and coalition operations. Though multinational interoperability is a work in progress, IN is working to establish memorandums of understanding, joint cooperation activities, and efforts such as Combined Endeavor and the Joint Warfighter Interoperability Demonstration initiatives that are held annually specifically for this purpose.

#### **Perpetuating Net-Centricity via JDEP**

Improving the ability to accurately represent system capabilities through models and simulations is key to Net-Centricity. The Joint Distrib-

See **INTEROPERABILITY** next page

# Defense Information Systems Agency

## Information sharing a top priority for DOD as it expands GIG

By DISA Staff

The duties of the Department of Defense are extensive and often extend to remote parts of the world. Therefore, communication is key. The Defense Information Systems Agency is directing its efforts toward aggressively expanding and enhancing the current end-to-end information transport system through its Global Information Grid Bandwidth Expansion, or GIG-BE, program.

GIG-BE is a major DOD net-centric transformational initiative to provide a secure, robust, optical terrestrial network that delivers very high speed classified and unclassified Internet Protocol services to key operating locations worldwide. By creating a ubiquitous "bandwidth-available" environment, GIG-BE is expected to offer improvements to national security intelligence, surveillance and reconnaissance and command and control information sharing.

The program, a joint venture with the Assistant secretary of defense- command, control, communications and Intelligence, will provide increased bandwidth and diverse physical access to approximately 90 critical sites in the Continental

United States, Pacific, and European theaters. These locations will be interconnected via an expanded GIG core.

ASD-C3I's vision for GIG-BE is a "color to every base," physically diverse network access, optical mesh upgrades for the backbone network, and regional/MAN upgrades, where needed. "A color to every base" implies every site will have an OC-192 (10 gigabits per second) of usable IP dedicated to that site.

Actual implementation of GIG-BE is expected to begin in late 2003. Engineers have surveyed more than 100 primary and alternate GIG-BE sites worldwide and have collected details on current and planned base infrastructure upgrades, commercial demarcation points and candidate locations for installation of service delivery nodes.

As of January, the GIG-BE Program Office has published and staffed recommendations for 104 bases. The few remaining bases are currently being addressed. The next steps toward implementation started in February, with detailed site engineering visits. The sequence of these installations is still subject to network design considerations.

---

### INTEROPERABILITY

*From previous page*

uted Engineering Plant within JITC is a joint funded system initiative that has been created to support systems engineering for Net-Centric based systems.

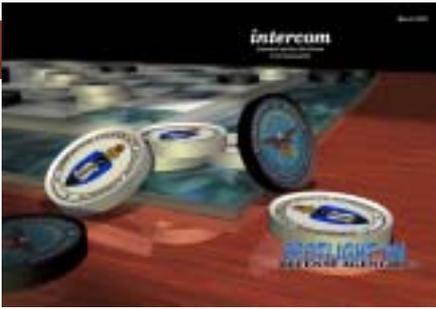
JDEP embodies the transformation tenets of NCW, providing DOD and industry with the means to examine the capabilities and limitations of existing systems for both warfighting and training purposes. It focuses on supporting both the end-user and systems developer, enabling them with the ability to test and evaluate interoperability among systems, i.e., assess the operational capabilities of forces via state of the art technologies (e.g., HLA, simulations, etc.).

Transitioned to JITC with programmatic oversight and responsibility in August 2002, it is anticipated that formal coordination and open dialogue with OSD, the defense agencies, services, and

industry will continue to grow, expanding on the concept of NCW as JDEP continues to mature.

Net-Centricity has made the overall objective of attaining interoperability on behalf of the warfighter more achievable now than ever before. It is a new concept that promotes continuity of effort, capitalizing on emerging, as well as existing efforts and initiatives. Needless to say, providing every type of capability as outlined is by no means trivial. However, from an organizational perspective, the NCW transformation paradigm when implemented can convert overwhelming technical challenges of the past, into golden opportunities that will benefit all of DOD today.

*Frank M. Holderness, a member of the Senior Executive Service, is the principal director for Interoperability within DISA. He is responsible for the development, adoption, specification, and certification of IT standards within DOD to ensure life-cycle interoperability and integration requirements are satisfied.*



## Defense Information Systems Agency

'New ways of thinking' with net-centric enterprise services

By DISA Staff

The need and importance of information in warfare is not new; what *is* new is the phenomenal increase in the amount of information needed. As Secretary of Defense Donald Rumsfeld said Jan. 30 of last year, " ... a revolution in military affairs is about more than building new high tech weapons ... it's also about new ways of thinking, and new ways of fighting."

The Defense Information Systems Agency is at the forefront of this effort to create new ways of thinking and fighting. Net-Centric Enterprise Services is a proposed program that would provide DOD components cutting-edge Web-based, networked applications to bridge real-time and near-realtime communities of interest, or COI.

NCES should ultimately provide ubiquitous access to reliable decision-quality information. NCES enables the end user to execute an intelligent pull of mission-tailored information from anywhere within the network environment with minimal latency, thus ensuring timeliness and relevance of the data.

NCES is a major initiative at DISA; the Agency anticipates that the program's products will change the way warfighters receive and process information. NCES will allow all echelons to better use the DOD network for the rapid decision processing necessary to support operations anywhere, anytime, by any user with network privileges.

NCES users will be able to rapidly leverage COI data producers and their release of real time data to a global data repository for general consumption and decision-making. With information more readily available, users will be able to execute command and control more effectively and rapidly within a given theater of operations.

With NCES, users will also be able to access information to a multitude of appliances including dedicated workstations, laptops with Web browsers, personal digital assistants, cellular tele-

phones and embedded processors. NCES will focus on implementing an open community process, which may include open source, allowing developers the flexibility they need to configure the infrastructure.

The Core Enterprise Services include:

*Enterprise Systems Management (ESM)*—provides end-to-end performance monitoring, configuration management and problem detection and resolution for the Global Information Grid, as well as enterprise IT resource accounting and addressing (e.g., for people, systems, devices, etc.).

*Messaging*—Allows users to exchange information among other users or applications on the enterprise infrastructure (e.g., e-mail, message oriented middleware, AOL instant messenger, wireless services, alert services).

*Discovery*—Processes for discovery of information content or services that exploit metadata descriptions of enterprise IT resources stored in directories, registries, and catalogs, including search engines.

*Mediation*—Services that help broker, translate, aggregate, fuse or integrate data/metadata.

*Collaboration*—Allows users to work together and jointly use selected capabilities on the network (i.e., chat, online meetings, work group software etc.).

*User Assistant*—Automated "helper" capabilities that reduce effort required to perform manpower intensive tasks.

*Security*—Capabilities that address vulnerabilities in networks, services, capabilities or systems.

*Storage*—Physical and virtual places to host data on the network with varying degrees of persistence (e.g., archiving, COOP, content staging).

*Application*—Infrastructure to host and organize distributed online processing capabilities.

These and other capabilities will make NCES an invaluable resource to the DOD as it seeks new ways of thinking and fighting to meet the demands of this technology-driven era.

# Defense Security Cooperation Agency

Founded on a tradition of cooperation

The Defense Security Cooperation Agency, Arlington, Va., directs and oversees U.S. foreign military sales, foreign military financing programs, international military education and training programs, humanitarian assistance and demining.

Security Cooperation is founded on a tradition of cooperation between the United States and other sovereign nations with similar values and interests in order to meet common defense goals. It consists of a group of programs authorized by the U.S. Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act, as amended, and related statutes.

Foreign Military Sales and International Military Education and Training are two key programs included within Security Cooperation. DSAA is the principal DOD organization through which the Secretary of Defense carries out responsibilities for Security Cooperation.

Within DSAA, the Information Technology directorate maintains and operates assigned information systems that support DSCA and the entire Security Cooperation community, and develops and enhances information systems to deliver new business value to the Security Cooperation community. The majority of the directorate's focus is on the Defense Security Assistance Management System, or DSAMS, and similar systems, and the legacy systems that would be replaced as a result.

The IT directorate is composed primarily of the DSAMS Program Management Office. Its missions are to:

- \* Oversee the development and maintenance of DSAMS and two MILDEP legacy systems on behalf of the Army and Navy, respectively

- \* Oversee the Defense Security Assistance Development Center in Mechanicsburg, Pa.

- \* Manage the DSAMS software development contract)

- \* Oversee DISA data center operations for DSAMS and five large legacy systems

- \* Oversee the Security Assistance Network managed by DISAM, and the Supply Tracking and Repairable Return system managed by AFSAC

- \* Formulate and manage budgets in conjunction with the comptroller

- \* Provide support to related initiatives such as the DSCA Portal.

The IT directorate also:

- \* Provides support to the Case Execution Management Information System initiative

- \* Manages all local automation for DSCA Headquarters (including unclassified and classified networks, e-mail, IT inventory, PC training)

- \* Oversees multiple DSCA Headquarters systems

- \* Coordinates IT security issues, such as information vulnerability alerts

- \* Coordinates Web site practices

- \* Ensures conformance with a variety of DOD CIO and government-wide IT policy, regulations and legislation and produces IT quantitative analyses. (*DSCA Web site*)



## Defense Legal Services Agency

Legal advice and services

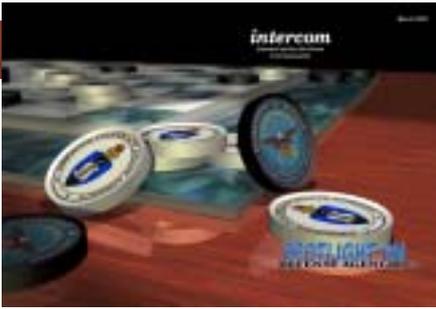
The Office of General Counsel in the Pentagon is headed by the General Counsel of the Department of Defense. The General Counsel is by law the Chief Legal Officer of DOD.

The General Counsel provides legal policy oversight and direction throughout the Department. He or she oversees, as appropriate, legal services delivered by the military and civilian attorneys in all DOD components. In addition, the General Counsel provides legal advice to the Secretary of

Defense, the Deputy Secretary of Defense and other Senior DOD officials.

The General Counsel is dual-hatted as the Director of the Defense Legal Services Agency, or DLSA, a DOD agency that provides legal advice and services for the defense agencies, DOD field activities, and other assigned organizations. The responsibilities and functions of the General Coun-

See DLSA Page 19



## Defense Logistics Agency

Quick, secure access to global inventories

The Defense Logistics Agency's mission is to provide best value logistics support to America's armed forces, in peace and war, around the clock, around the world. If service members eat it, wear it, drive it, shoot it, or burn it, chances are that DLA helps provide it. It also disposes of materiel and equipment that is no longer needed. All of this effort requires the work of 23,000 civilian and military employees. By using proven business practices and strategies, DLA is continually re-engineering, reinventing and reforming the way it does business to provide best value solutions to customers.

DLA is a defense agency. The DLA director reports to the under secretary of defense for Acquisition, Technology and Logistics through the deputy under secretary of defense (Logistics and Materiel Readiness). DLA provides worldwide logistics support for the missions of the military departments and the unified combatant commands under conditions of peace and war. It also provides logistics support to other DOD components and certain federal agencies, foreign governments, international organizations, and others as authorized. DLA's origins date back to World War II when America's huge military buildup required the rapid procurement of vast amounts of munitions and supplies.

DLA and its Information Operations office, J-6, have many exciting information technology initiatives under way that will improve support to warfighters by allowing quick, secure access to global inventories and industry surge capabilities to fully integrate customer and supplier information.

The foundation for this customer service improvement is its Business Systems Modernization initiative. BSM will allow DLA to replace mission-critical legacy systems with an enterprise business system based on commercially available off-the-

shelf software. BSM will allow DLA to adopt proven and successful business practices used in the commercial marketplace.

**Another major IT initiative is the Integrated Data Environment.** IDE will provide a DOD eBusiness information exchange service where a shared information capability enables common interactive business practices among military services, agencies, and their trading partners.

**Other IT initiatives are:**

**Knowledge Management.** DLA is actively implementing knowledge management practices by creating an environment where information sharing is encouraged and drives process improvement.

**Joint Total Asset Visibility.**

JTAV is the capability to provide users with timely and accurate information on the location, movement, status, and identity of units, personnel, equipment, and supplies. It facilitates the capability to act upon that information to improve overall performance of DOD's logistics practices (e.g., in-storage, in-process, in-transit).

**Electronic Business/Electronic**

**Commerce.** Develop, implement, and sustain common enterprise-wide eBusiness solutions that support strategic information exchange in the DOD by using commercial best business technologies and practices.

The J6 is DLA's knowledge broker, providing comprehensive, best practice technological support to the DOD/DLA logistics business community resulting in highest quality information systems, efficient and economical computing, data management, electronic business, and telecommunication services.

The J-6 organization consists of:

See DLA next page



**DLSA**  
From Page 17

sel in his or her capacity as the Director, DLSA, include:

Organize, direct, and manage the DLSA and all assigned resources.

Provide legal advice and services to the defense agencies, DOD field activities, and other assigned organizations.

Provide technical support and assistance for development of the DOD Legislative Program.

Manage the Departmental legislative comment programs.

Provide a centralized legislative document reference and distribution point for the DOD and maintain the Department's historical legislative files.

Coordinate DOD policy for standards of con-

duct and administer the Standards of Conduct Program for the OSD and other assigned organizations.

Administer the Security Clearance Review Program.

DLSA includes the following:

The Standards of Conduct Office, which advises officials in OSD and elsewhere in the Department of their obligations under the government ethics regulations;

The Legislative Reference Service, which is responsible for coordinating all legislative proposals within DOD and, through the Office of Management and Budget, the Executive Branch; and

The Defense Office of Hearings and Appeals, the largest component of DLSA, which provides hearing and appeal procedures for security clearance determinations, CHAMPUS determinations, and other matters.

---

**DLA**  
From previous page

**Program executive officer.** Single agency official providing overall direction and guidance for development, acquisition, testing, systems integration, product improvement, and fielding of assigned DLA programs while maximizing Return on Investment and contribution to DLA's mission outcome through portfolio management and oversight.

**Technology services and infrastructure support.** Responsible for managing the agency's information technology infrastructure. IT infrastructure includes all of the hardware and software components that provide secure, interoperable computing solutions for supporting DLA's mission. Components include: workstations, servers, firewalls, local area networks, wide area networks, telecommunications and the operating systems and other software used to efficiently and effectively operate, manage, and maintain the infrastructure.

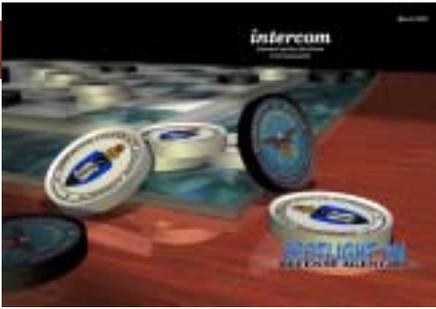
**Enterprise business systems.** Provides program management oversight, automated information systems administration, application development including Web design and development, maintenance of the operational architecture, and while managing strategic direction of the DLA business systems.

**IT policy, plans & assessment directorate.** Responsible for developing DLA-wide IT policies, planning, and assessments on IT investments, pro-

cesses, and policy adherence, focusing specialized expertise on: technical architecture, information assurance, infrastructure protection, investment processes, records management, knowledge theft, emerging technologies, and the review and coordination of functional requirements.

**JECPO/eBusiness.** Responsible for providing robust electronic business and commerce services in support of both the DLA and DOD missions by using commercial best business technologies and practices. Provides enterprise-wide electronic business services that support DLA and DOD strategic objectives to include: integrated data environment; document automation and production services; cataloging and product data dissemination; management of DOD logistics transactions and their corresponding business rules; total asset visibility and situational awareness for DOD/DLA items; and automatic identification technology standards.

**Business management office.** Principal advisors to the executive director, J-6, and the J-6 executive team for administration and management of J-6 business functions which include programming, budgeting and resource management, contract review and assessment, workforce development, internal management controls, compliance, J-6 communications, administrative databases and repositories, space management, inventory tracking and general orders. (*DLA Web site*)



## Defense Security Service



Safeguarding our nation's security

The Defense Security Service, formerly the Defense Investigative Service, plays a crucial role in safeguarding our nation's security. As a DOD agency, DSS makes its contribution to the national security community by conducting personnel security investigations and providing industrial security products and services, as well as offering comprehensive security education and training to DOD and other government entities. To complement its three primary missions: the Personnel Security Investigations Program, the Industrial Security Program; and the Security Education, Training and Awareness Program, DSS offers the unique advantage of integrating counterintelligence into its core security disciplines through training programs, policy development, and operational support to field elements.

The mission of DSS is realized through the efforts of approximately 2,600 employees strategically located throughout the United States and Puerto Rico. Almost one half of the DSS workforce is comprised of special agents who accomplish about 500,000 personnel security investigations each year. Another 230 DSS employees are industrial security representatives who oversee, advise and assist more than 11,000 contractor facilities involved with classified contracts and research/development efforts.

### **Personnel Security Investigations Program**

DSS administers one of the most comprehensive PSI programs offered in the defense industry. The "background investigations" conducted by special agents on DOD military, civilian and contractor personnel are used to determine an individual's suitability to enter the armed forces, access classified information, or hold a sensitive position within DOD.

### **Personnel Investigations Center**

Personnel security investigations are submitted to the PIC where they are opened, processed and closed upon completion. The final investigative report is forwarded to the appropriate DOD

adjudicative facility. This operating center is at Fort Meade, Md.

### **Industrial Security Program**

In addition to the PSI program, DSS administers three industrial security programs, of which the National Industrial Security Program is the largest. Under the NISP, DSS industrial security representatives oversee cleared contractor facilities and assist the organizations' management staff and facility security officers in formulating their security programs. The remaining two DSS industrial security programs, the Arms, Ammunition and Explosives Program and the Critical Infrastructure Program provide protection for arms, ammunition and explosives and DOD critical assets and infrastructure, respectively.

### **Defense Industrial Security Clearance Office**

The DISCO, in Columbus, Ohio, processes, issues and maintains industrial security program facility clearances and industrial security personnel security clearances.

### **Security, Education, Training and Awareness**

Security education, training, professional development support, and counterintelligence awareness is the third major mission area of DSS.

### **Defense Security Service Academy**

The DSS Academy, in Linthicum, Md., trains almost 10,000 students within the DOD and defense industry each year. Through formal classroom training, computer-based training, correspondence/distance learning and tele-training, the Academy provides a curriculum focusing on the core security disciplines while integrating counterintelligence and information systems security.

### **DSS counterintelligence office**

The Counterintelligence Office, established in May 1993, integrates CI with the DSS three core mission areas; infusing CI experience and knowledge throughout the workforce; increasing CI awareness throughout DSS and industry; and

See **DSS** next page

# Defense Threat Reduction Agency

## Making the world safer by reducing the threat of WMD

The mission of the Defense Threat Reduction Agency is to make the world safer by reducing the threat of weapons of mass destruction. The Defense Threat Reduction Agency pursues its mission by employing a set of five tools.

The first tool, *arms control inspections*, is employed to verify that other nations are abiding by the treaties that they signed. This enables U.S. leadership to make informed decisions about defense investments.

When DTRA personnel are unable to verify the lack of weapons of mass destruction, the second tool, *cooperative threat reduction*, is employed. The goal of the CTR program is to use cooperative means to destroy weapons of mass destruction threats. CTR has successfully dismantled more than 5,000 missiles from their warheads. Although the warheads have not been destroyed, they now lack delivery systems. Due to the CTR program, Belarus, Kazakhstan, and Ukraine are nuclear weapon-free.

If agency personnel are unable to verify the lack of WMD, and are unable to cooperatively eliminate existing weapons, *uncooperative threat reduction - technology development* - can be employed. Uncooperative threat reduction refers to developing and delivering precision-guided weapons to destroy weapons of mass destruction threats. Thermobaric weapons and global positioning satellite-guided weapons that DTRA has provided to/developed for combatant commanders are two examples of uncooperative threat reduction successes.



The fourth tool is *chemical and biological defense*. This tool helps DTRA manage the nation's defense against WMD.

Lastly, *combat support* assesses vulnerabilities as a service to the warfighter. Combat support includes assessing the viability of deterrents, vulnerability assessments, and consequence assessments. DTRA carries out its mission of stewardship over the U.S. nuclear arsenal and works to assure the security of military facilities abroad.

As a combat support agency, DTRA serves the combatant commanders, the services, the Department of Defense, and other agencies, as appropriate. The agency is led by Dr. Stephen M. Younger who reports to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs. DTRA is comprised of more than 2,000 personnel coming from the military services, the federal civil service, universities, non-governmental organizations, and corporate America.

With personnel at more than 14 locations around the world, DTRA is organized by mission essential directorates (Chemical-Biological Defense, Combat Support, Cooperative Threat Reduction, On-Site Inspection, and Technology Development) and enabling directorates (Acquisition and Logistics, Information Management, Resource Management, and Security and Counterintelligence) to effectively carry out the agency's goals and objectives. (See next page)

---

### DSS

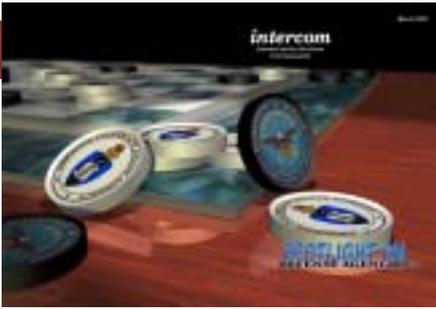
*From previous page*

assisting customers in recognizing and reporting suspected foreign intelligence collection activities. The main thrust of the DSS CI program has been to train and sensitize industry and DSS personnel to recognize CI indicators, look for suspicious events in today's rapidly changing threat environment, and provide timely reporting of such information.

The DSS industrial security information assurance branch is comprised of computer security spe-

cialists and computer scientists who support existing industrial security programs. This support includes AIS certification and accreditation of cleared contractor facilities; IA awareness and security training of contractor security personnel; administrative inquiry assistance; and consultation on AIS issues.

Computer technology is rapidly evolving and with every change comes the increased potential for vulnerability. We must stay informed regarding how these changes affect the protection of information systems and the data stored within them. (*DSS Web site*)



## *Defense Threat Reduction Agency*

### Computer-modeling systems predict disaster effects

DTRA's Technology Development directorate is responsible for developing, testing, and fielding offensive and defensive technologies designed to counter the proliferation of weapons of mass destruction. The directorate serves as the near-term interface between research and development and the warfighter. One of the directorate's notable successes has been development and distribution of the Hazard Prediction and Assessment Capability, or HPAC, program and the Consequence Assessment Tool Set, or CATS. These computer-modeling systems allow personnel in the field to forecast the effects of unpredictable phenomena such as natural or man-made disasters.

DTRA also supplies reach-back capabilities for both HPAC and CATS. Customers can contact either the Consequence Assessment branch of the Technology Development directorate or the DTRA operations center to request quality control checks on analyses run by customers, or to ask DTRA to run HPAC and CATS reports to order.

#### **Consequences Assessment Tool Set**

CATS is a consequence management tool package that integrates hazard prediction, consequence assessment, emergency management tools, including the Hazard Prediction and Assessment Capability system, and critical population and infrastructure data within a commercial Geographical Information System. The GIS interface enables the user to combine and manipulate multiple layers of information on a variety of visual information backgrounds and maps to assess affected persons, property and infrastructure. Through user-friendly graphical interfaces and pre-defined event scenarios, CATS can be used regardless of the user's level of expertise or access to information.

The DTRA and the Federal Emergency Management Agency developed CATS to support emer-

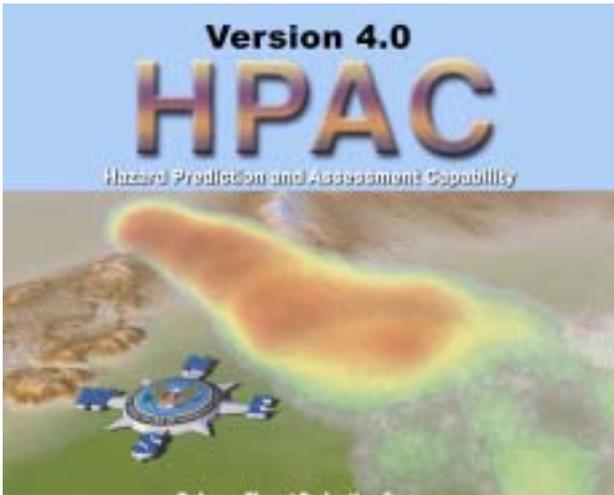


**DTRA and the Federal Emergency Management Agency developed the CATS tool set.**

gency managers' training, exercises, contingency planning and logistical planning as well as to calculate requirements for humanitarian aid and force protection. The functional utility of the CATS system begins with the ability to predict the shape of hazard areas caused by earthquakes, hurricanes or chemical, biological, radiological, nuclear or explosive events. In these situations, the CATS system can assess resultant casualties and damage to facilities, resources and infrastructure, as well as estimate collateral damage to military, civil and industrial installations. The system also creates mitigation strategies for both tactical and strategic force support.

#### **Hazard Prediction and Assessment**

Operation Desert Storm illustrated the need for an automated hazard prediction tool. During that campaign, predictions of the collateral effects of potential weapons of mass destruction use were inefficient and untimely. Predictions were con-



The Hazard Prediction and Assessment Capability is an automated software system.

ducted by sending requests for analysis from the theater of operations to the Defense Nuclear Agency (a predecessor organization to the DTRA) for technical analysis. Analytical products were then sent back to the theater. This experience prompted the effort to make hazard prediction and collateral effects tools available in the theater of operations. DTRA's background of more than 50 years of research blast effects and analysis provided a strong platform to accomplish this mission.

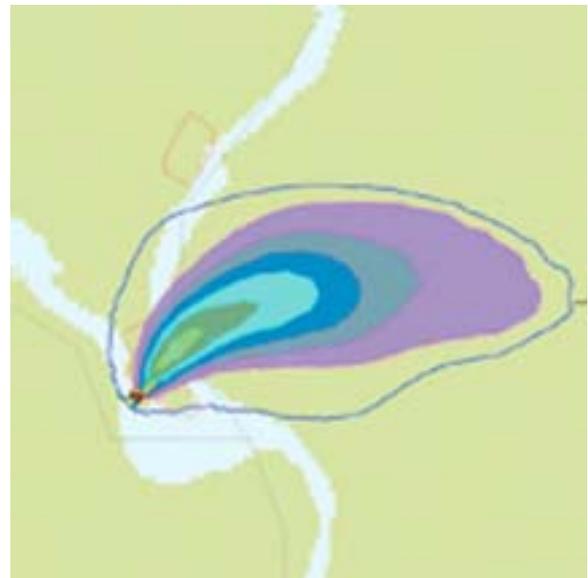
The HPAC automated software system, a forward-deployable counterproliferation-counterforce collateral assessment tool, provides the means to accurately model nuclear, biological, chemical, radiological, and high explosive collateral effects resulting from conventional weapon strikes against enemy weapons of mass destruction production and storage facilities. The HPAC system also predicts downwind hazard areas resulting from a nuclear weapon strike or reactor accident and has the capability to model nuclear, chemical and biological weapon strikes or accidental releases. The system uses integrated source terms, high-resolution weather forecasts and particulate transport analyses to model hazard areas produced by military or terrorist incidents and industrial accidents.

Relevant real-world hazard prediction requires

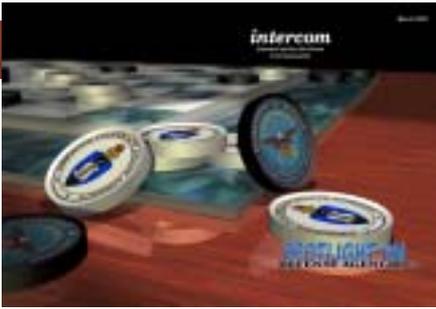
timely and accurate weather data in the area of concern. The HPAC system allows the user easy access to weather forecasts and real-time weather observation data by using a variety of DTRA supported meteorological data server systems. The HPAC system also has embedded climatology or historical weather data for planning incidents beyond the normal time associated with credible forecast weather data. One-kilometer terrain data and supporting wind-flow models calculate the local winds field in the area of concern. Other weather sources are also available upon request to DTRA.

The HPAC system can also help answer the question, "How good is the prediction?" by providing probabilistic calculations. The hazard area feature estimates the weather uncertainty and turbulence effects on possible plume trajectories and calculates the areas of hazard impact and the degree of confidence of the prediction.

The interoperable CATS and HPAC computer modeling systems are vital tools that equip personnel on the ground with real-time modeling, communications, and assessment capabilities.



A map generated by Defense Threat Reduction Agency-developed software shows the area affected by a simulated biological weapon attack.



## *Defense Threat Reduction Agency*

### Tools give warfighter real-time collaboration and situational awareness

DTRA's Technology Development directorate serves as the near-term interface between research and development and the warfighter. One of the directorate's current efforts is to customize and integrate two products developed to provide real-time collaboration and situational awareness capabilities in support of the warfighter. These products are the Defense Collaboration Tool Suite, or DCTS, and the Area Security Operations Command and Control, or ASOCC, system. The Operational Applications branch of the Technology Development directorate is working to customize and integrate these tools into DTRA's incident identification and response capabilities.

#### **Defense Collaboration Tool Suite**

The Defense Collaboration Tool Suite was developed to provide a standard set of tools to solve interoperability problems among the combatant commanders, services, agencies and allied forces. It is an MS Windows-based, Internet-enabled collaboration standard that provides voice and video conferencing, instant messaging, file and application-sharing, streaming media, and shared whiteboard capabilities to multiple users in a real-time environment. Most of the components are off-the-shelf, increasing users' familiarity and ease of use.

DTRA participated in the Advanced Technology Concept Demonstrations sponsored by Pacific Command in August 2000 to evaluate DCTS and is developing a customized version of the DCTS standard for use within DTRA. DTRA's goal is to develop a DCTS that will support the warfighter anytime, anywhere. The customized system will allow DTRA personnel or warfighters using DTRA's analytical tools to connect through a computer terminal to a real-time collaborative computing environment with DTRA headquarters. This will give forward deployed assets full access to DTRA's analytical capabilities and software packages, as well as the ability to ask questions and receive immediate feedback to ensure the most

accurate communication of information in critical situations.

#### **Area Security Operations C2 System**

The Area Security Operation Command and Control System, or ASOCC, developed by the Homeland Security Advanced Technology Concept Demonstration, is an automated, interactive computer-based application designed to provide near real-time situational awareness to commanders and collaborative planning capabilities for use with civil authorities. Unlike DCTS, ASOCC is a specialized application that runs on computer workstations and provides specific command and control functions. The program shows the near-real time security status of participating sites and immediately sends updates to all computers linked to the system through the Internet or a local area network.

DTRA is integrating ASOCC with other DTRA analytical products for use in developing a common operational picture among warfighters, first responders and other critical personnel in crisis situations. Specifically, by integrating ASOCC and DCTS, DTRA personnel and others can use DCTS to update ASOCC and transmit time-critical security warnings through a collaborative network. DTRA is working with the Homeland Security Command and Control ATCD to evaluate ASOCC's military utility.

DTRA's successful integration of DCTS and ASOCC into its analytical tool-set will augment response capabilities to weapons of mass destruction-related incidents in the homeland and in the field. Both are vital tools that equip personnel on the ground with real-time or near real-time collaboration and operational information. The interoperability of these systems creates a powerful, integrated Web of information exchange that will revolutionize the relationship of personnel on the ground, their central command structures, and the civil sector for use in operational or crisis planning situations.

# Defense Threat Reduction Agency

## Enterprise architecture program provides roadmap to 21st century

The mission of the Information Management directorate is to provide an effective infrastructure (people, policies, procedures and technology) that allows secure and continuous sharing of information among DTRA members and their customers. IM accomplishes this by leveraging information technology to enhance internal and external communications, knowledge sharing and mission performance.

### Shaping DTRA's IT Systems

Under the leadership of Information Management, DTRA is implementing an enterprise architecture, or EA, program. An effective EA program will create an agency-wide roadmap to enhance the agency's ability to achieve its mission through optimal performance of core business processes within an efficient and effective information technology environment. Agencies are required to develop EA programs by the federal government to reduce the risk of building information technology systems that are duplicative, incompatible, and unnecessarily costly to maintain and integrate. The overriding goal of DTRA's EA program is to help the agency increase its ability to support the warfighter, in particular through providing the IT tools necessary to aid the e-enabled warfighter. At the same time, IM's challenge is to maintain existing systems, inherited from varied and diverse legacy stovepipe architectures, while moving to an interim architecture that will eventually culminate in the fully formed DTRA enterprise architecture.

The enterprise architecture program can be described as a snapshot of the current DTRA business and IT environment, as well as a process or a blueprint for systematically and completely achieving DTRA's business process enhancements and information goals. The objectives of DTRA's EA program include: establishing interoperability standards; coordinating technological investment with business architecture; minimizing data collection burdens; securing information against unauthorized access; advancing the standardization of common functions and customers; providing greater access of information, as appropriate; selecting and implementing proven technology; all while fully complying with the DOD and federal laws and statutes.

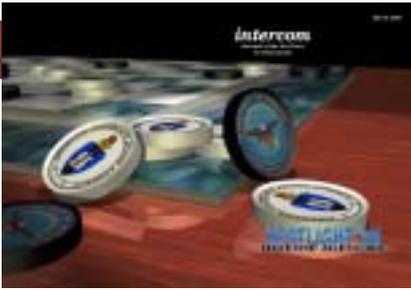


Defense Threat Reduction Agency

### Mission Enhancement through Improved EA

While pursuing these objectives, the EA program will enable and support DTRA's mission. The EA program enhances decision support and provides reliable, interoperable, flexible and secure information, and eventually knowledge, for agency operations. Many of DTRA's most critical mission support products and tools are computer-based and provided online within the agency and to warfighters and DTRA personnel in the field. A thorough and successful EA program will allow IM to identify DTRA's core processes and build the enterprise architecture to deliver information technology as efficiently and effectively as possible. The EA program also provides a process with measurable objectives and provides for efficient IT investments by capturing DTRA-wide current capabilities, facilitating planned enhancements, eliminating unnecessary duplication, and enabling effective and efficient IT investments. The DTRA EA program ensures the infrastructure remains responsive to the business and technology needs of the agency, and to those people that fulfill its mission requirements.

The EA program is a continuing process, where success is determined over time as the infrastructure is modernized and users are continuously surveyed to ascertain or verify that their needs are being met. Satisfaction of objectives is also enhanced through a process that continually surveys technology sources to identify new and improved technologies, concepts and products that can be included in the infrastructure to improve performance, reliability, security and capabilities.



## Missile Defense Agency

Mission: Protect nation from missile attack

The Missile Defense Agency's mission is to develop, test and prepare for deployment a missile defense system. Using complementary interceptors, land-, sea-, air- and space-based sensors, and battle management command and control systems, the planned missile defense system will be able to engage all classes and ranges of ballistic missile threats. The programmatic strategy is to develop, rigorously test, and continuously evaluate production, deployment and operational alternatives for the ballistic missile defense system. Missile defense systems being developed and tested by MDA are primarily based on hit-to-kill technology. It has been described as hitting a bullet with a bullet – a capability that has been successfully demonstrated in test after test.

While the end of the Cold War signaled a reduction in the likelihood of global conflict, the threat from foreign missiles has grown steadily as sophisticated missile technology becomes available on a wider scale. The proliferation of weapons of mass destruction and the ballistic and cruise missiles that could deliver them pose a direct and immediate threat to the security of U.S. military forces and assets in overseas theaters of operation, our allies and friends, as well as our own country. At least 25 countries now possess – or are acquiring – nuclear, biological and chemical weapons. Since 1980, ballistic missiles have been used in six regional conflicts. During the Gulf War, 28 U.S. service personnel died from an Iraqi SCUD missile attack.

In light of the new security environment and progress made in missile defense development efforts, the president directed the DOD to begin fielding initial missile defense capabilities in 2004-2005 to meet the near-term ballistic missile threat to our homeland, our deployed forces, and friends and allies. These initial capabilities emerge from our research and development program and build on the test bed we have been constructing.

The DOD is employing an evolutionary approach to the development and deployment of missile defenses over time. The composition of missile defenses, including the number, type and location of systems deployed, will change over time to meet the changing threat and take advantage of technological developments.

The initial set of capabilities planned for 2004-2005 will include: ground-based interceptors that can destroy intercontinental ballistic missiles during the midcourse phase of flight; sea-based interceptors employed on existing Aegis ships to intercept short and medium range ballistic missiles in the mid-course phase of flight; deployment of air-transportable Patriot Advanced Capability-3 systems to intercept short and medium range ballistic missiles; land, sea and space-based sensors, including existing early warning satellites, an upgraded radar at Shemya, Alaska, a new sea-based X-band radar, and other sensors now on Aegis cruisers and destroyers.

Because the threats of the 21st century also endanger our friends and allies around the world, it is essential that we work together to meet these threats. The Department of Defense plans to develop and deploy missile defenses capable of protecting not only the United States and our deployed forces, but also friends and allies. The missile defense program will be structured in a way that encourages industrial cooperation by friends and allies, consistent with overall U.S. national security.

The deployment of missile defenses is an essential element of overall national security policy to transform U.S. defense and deterrence capabilities to meet emerging and evolving threats. The evolutionary approach to missile defense provides near-term capability as we continue to pursue a robust research and development program against ballistic missiles of all ranges. *(MDAlink)*



**MDA** interceptor launch.

# National Imagery and Mapping Agency

## **Vision: Know the Earth ... Show the Way**

NIMA was established by the National Imagery and Mapping Agency Act of 1996. Because it has responsibilities to customers outside DOD, NIMA has also been designated a part of the U.S. intelligence community.

The creation of NIMA centralized responsibility for imagery and mapping, representing a fundamental step toward achieving the DOD vision of “dominant battle space awareness.” NIMA was created to better exploit the tremendous potential of enhanced collection systems, digital processing technology and the prospective expansion in commercial imagery than its separate predecessor organizations.

With headquarters in Bethesda, Md., NIMA operates major facilities in the northern Virginia, Washington, D.C., and St. Louis, as well as support and liaison offices worldwide.

NIMA provides geospatial intelligence in all its forms, and from whatever source – imagery, imagery intelligence, and geospatial data and information – to ensure the knowledge foundation for planning, decision and action. It provides easy access to geospatial intelligence databases for all stakeholders and creates tailored, customer-specific geospatial intelligence, analytic services, and solutions.

NIMA is organized around its core business processes to enable the agency to take advantage of horizontal teaming and integration activities to draw the producers and consumers of NIMA’s information closer together.

NIMA brought together the Defense Mapping Agency, the Central Imagery Office, and the Defense Dissemination Program Office in their entirety; and the mission and functions of CIA’s National Photographic Interpretation Center. Those organizations were disestablished Oct. 1, 1996. Also included in NIMA are imagery exploitation, dissemination and processing elements of the Defense Intelligence Agency, National Reconnaissance

Office and the Defense Airborne Reconnaissance Office.

The NIMA work force is populated by professionals in fields such as cartography, imagery analysis, marine analysis, the physical sciences, geodesy, computer and telecommunications engineering, and photogrammetry.

## **Major Organizations**

The Analysis and Production directorate provides geospatial intelligence and services to policymakers, military decision-makers and warfighters, and tailored support to civilian federal agencies and international organizations. This geospatial intelligence is derived from many sources. The directorate supports NIMA’s goal to ensure a knowledge foundation for planning, decisions and action.

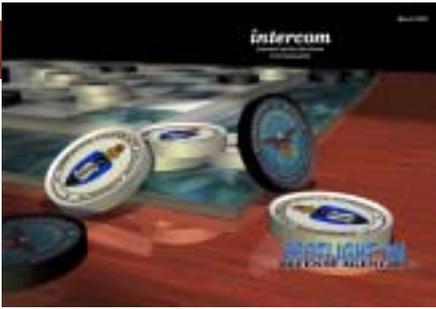
The Acquisition directorate enables, acquires and provides systems, supplies, services and business solutions. The directorate is responsible for acquisition of systems that advance a national leadership role in the imagery, imagery analysis, and geospatial information communities. The directorate focuses on pre-acquisition studies; the acquisition program; systems engineering; and the advancement of systems engineering, acquisition/contracting, infrastructure engineering, and imagery and



**Satellite view of Washington**

geospatial sciences.

The InnoVision directorate forecasts future environments, defines future needs, establishes plans to align resources, and provides technology and process solutions to lead NIMA, its customers and partners into the future. InnoVision also provides the focal point in NIMA to address the future, leads NIMA into the future by developing comprehensive plans and technology initiatives based on analysis of intelligence trends, technology advances, and emerging customer and partner concepts, drives NIMA transformation by linking needs, analysis, plans, advanced technologies, programs and resources, and champions the transformation of the intelligence community. (*NIMA Web site*)



## *National Security Agency*

Protects U.S. info, produces foreign intel

The National Security Agency, at Fort George Meade, Md., is the nation's cryptologic organization. It coordinates, directs and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. A high technology organization, NSA is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the government.

Signals intelligence, or SIGINT, is a unique discipline with a long and storied past. SIGINT's modern era dates to World War II, when the U.S. broke the Japanese military code and learned of plans to invade Midway Island. This intelligence allowed the U.S. to defeat Japan's superior fleet. The use of SIGINT is believed to have directly contributed to shortening the war by at least one year. Today, SIGINT continues to play an important role in maintaining the superpower status of the U.S.

As the world becomes more and more technology-oriented, the information systems security, or INFOSEC, mission becomes increasingly challenging. This mission involves protecting all classified and sensitive information that is stored or sent through U.S. government equipment. INFOSEC professionals go to great lengths to assure government systems remain impenetrable. This support spans from the highest levels of U.S. government to the individual warfighter in the field.

NSA conducts one of the U.S. government's leading research and development programs. Some

of the Agency's R&D projects have significantly advanced the state of the art in the scientific and business worlds. NSA's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to the modern computer. NSA pioneered efforts in flexible storage capabilities, which led to the development of the tape cassette. NSA also made ground-breaking developments in semiconductor technology and remains a world leader in many technological fields.

NSA employs the country's premier codemakers and codebreakers. It's said to be the largest employer of mathematicians in the U.S. and perhaps the world. Its mathematicians contribute directly to the two missions of the agency: designing cipher systems that will protect the integrity of U.S. information systems and searching for weaknesses in adversaries' systems and codes.

Most NSA employees, both civilian and military, are headquartered at Fort Meade. Its work force represents an unusual combination of specialties: analysts, engineers, physicists, mathematicians, linguists, computer scientists, researchers, as well as customer relations specialists, security officers and data flow experts, managers, and administrative and clerical assistants.

*The ability to understand the secret communications of our foreign adversaries while protecting our own communications — a capability in which the United States leads the world — gives our nation a unique advantage. (NSA Web site)*

## *Pentagon Force Protection Agency*

### **The Pentagon's Police**

In response to the terrorist attack against the Pentagon on Sept. 11, 2001, the Department of Defense established the Pentagon Force Protection Agency. The new agency absorbed the Pentagon's police force, formerly known as the Defense Protective Service, and its role of providing basic law enforcement and security for the Pentagon and

DOD interests in the National Capital Region.

PFPA expanded that mission to provide force protection against the full spectrum of potential threats through robust prevention, preparedness, detection and response measures. The agency provides those services to the 280-acre "Pentagon Reservation" as well as numerous other DOD activities and facilities within the NCR.

## Lt. Gen. Winston Powers Former DCA director passed away Feb. 6

An early leader of the Air Force communications and information community, retired Lt. Gen. Winston D. Powers, died Feb. 6, from advanced diabetes and congestive heart failure. Powers' last assignment was as the director of the Defense Communications Agency in Washington. He served there from 1983 to 1987, responsible for the management of the worldwide Defense Communications System.

Born in 1930, he enlisted in the Air Force in 1950. Volunteering for navigator training, he was sent to Ellington AFB, Texas, graduating in 1953. After combat crew training he went back to Ellington as a navigator instructor.

In 1957, he entered the Tactical Communications Officer Training School at Scott AFB, Ill. After graduation, he became commander of Detachment 2, 6123rd Air Control and Warning Squadron, in South Korea. He returned to Scott in 1959 at the 1918th Communications Squadron.

Under Operation Bootstrap, he graduated from McKendree College in 1961, and was assigned to the Air Force Command Post as a communications officer. In 1963, he was selected to attend the communications system engineering program of the American Telephone and Telegraph Company in New York City. In 1964 he became a communications engineer for DCA-United Kingdom.

He transferred to the Tactical Communications Area at Langley AFB, Va., in 1967. He returned to a flying assignment in 1970 with the 460th Reconnaissance Wing at Tan Son Nhut AB, Vietnam. He flew 75 combat missions in EC-47s.

From 1971 to 1973, he was assigned to the Joint Chiefs of Staff in the Plans and Policy division, J6. He moved to Air Force headquarters as special assistant for joint matters in the directorate of Command, Control and Communications, office of the deputy chief of staff, Programs and Resources.

Returning to South Korea in 1974, he was commander of the 2146th Communications Group and director of communications-electronics for the 314th Air Division at Osan AB. In November 1974, he was assigned to Air Force headquarters, directorate of Command, Control and Communications.



Lt. Gen. Winston D. Powers

He became deputy director of telecommunications, and command and control resources, office of the assistant chief of staff, Communications and Computer Resources, Air Force headquarters in 1975 and later became director. In July 1978, he was appointed deputy director of command,

control and communications.

He transferred to Peterson AFB, Colo., in October 1978, serving first as the deputy chief of staff for Communications, Electronics and Computer Resources for the North American Aerospace Defense Command and U.S. Aerospace Defense Command. He became chief of the Systems Integration Office, Headquarters Aerospace Defense Center in 1981, and took command of the Space Communications Division at Peterson AFB in 1983. He served there until becoming director of the DCA.

After retiring, he held several consulting jobs, including vice president for business development at McDonnell Douglas Electronic Systems Co. in McLean, Va.

In noting the changes that had occurred during his career, the general, in a prescient view of the future, said in an interview that the battlefield of the future would be "totally dependent on embedded computer systems." To balance this, he pointed out that the Air Force would need "bright people, trained in new skills and disciplines, to exploit those opportunities." In comments just as relevant today as when they were written, he warned the communicators not to become "too 'macro' in their thinking." He said, "Sensitivity to the operational mission and the supported operational commanders is required to see the forest for the trees."

Powers was inducted into the Air Force Communications and Information Hall of Fame, Class of 2000.

# AFNOSC transforms Air Force enterprise command and control

By 1st Lt. Reid Novotny, 1st Lt. James Hudson, and 2nd Lt. Steven Pressley  
COMAFFOR CNO Operations Center  
Barksdale AFB, La.

The Air Force has always been on the cutting edge of computer technology. We have great organizations that keep us abreast of rapidly evolving innovations. Currently the Air Force Computer Emergency Response Team defends our networks, and the Air Force Network Operations Center enables our information flow. Base network control centers reporting to the major command network operations and security centers are the gatekeepers for information flow within the MAJCOM. To truly employ information superiority, the Air Force requires one organization to unite these nine MAJCOM NOSCs, as well as other communications agencies to provide a single command and

control authority. This is where the Air Force Network Operations and Security Center enters the fight. The AFNOSC is being built at 8th Air Force Headquarters, Barksdale AFB.

The Air Force computer network enterprise is composed of a loose federation of MAJCOM NOSCs with several DOD and Air Force communications agencies acting as directors and advisors. See Figure 1.

Several problems arise from the current organizational structure of the Air Force Network. The differentiation between service-specific and joint/component responsibilities causes command and control disconnects. Information assurance and Enterprise Network Operations are the job of the Air Force, but there is also a need for an organization to act as the service component to the Joint Task Force for Computer Network Operations. The 8th Air Force vice commander is designated as the

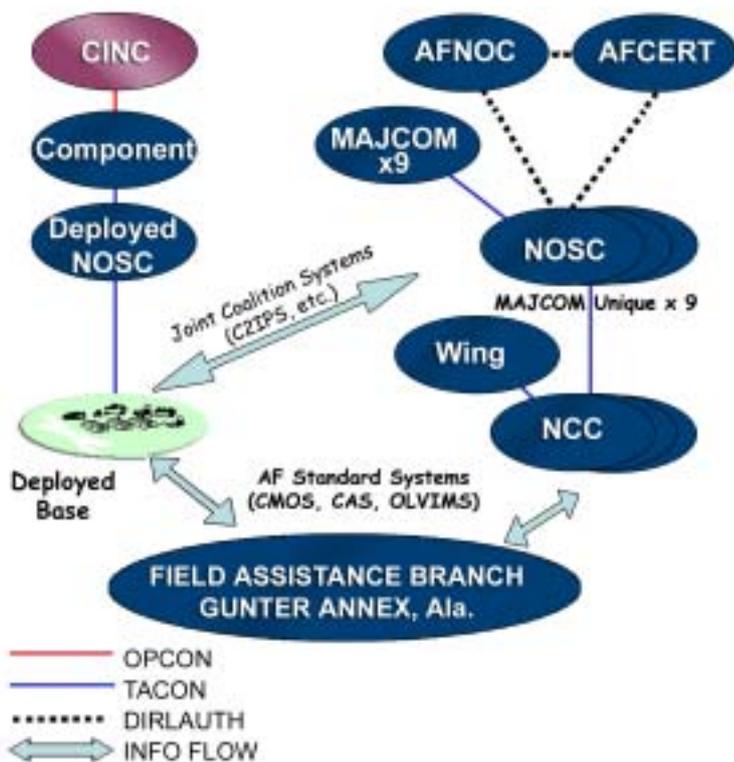


Figure 1

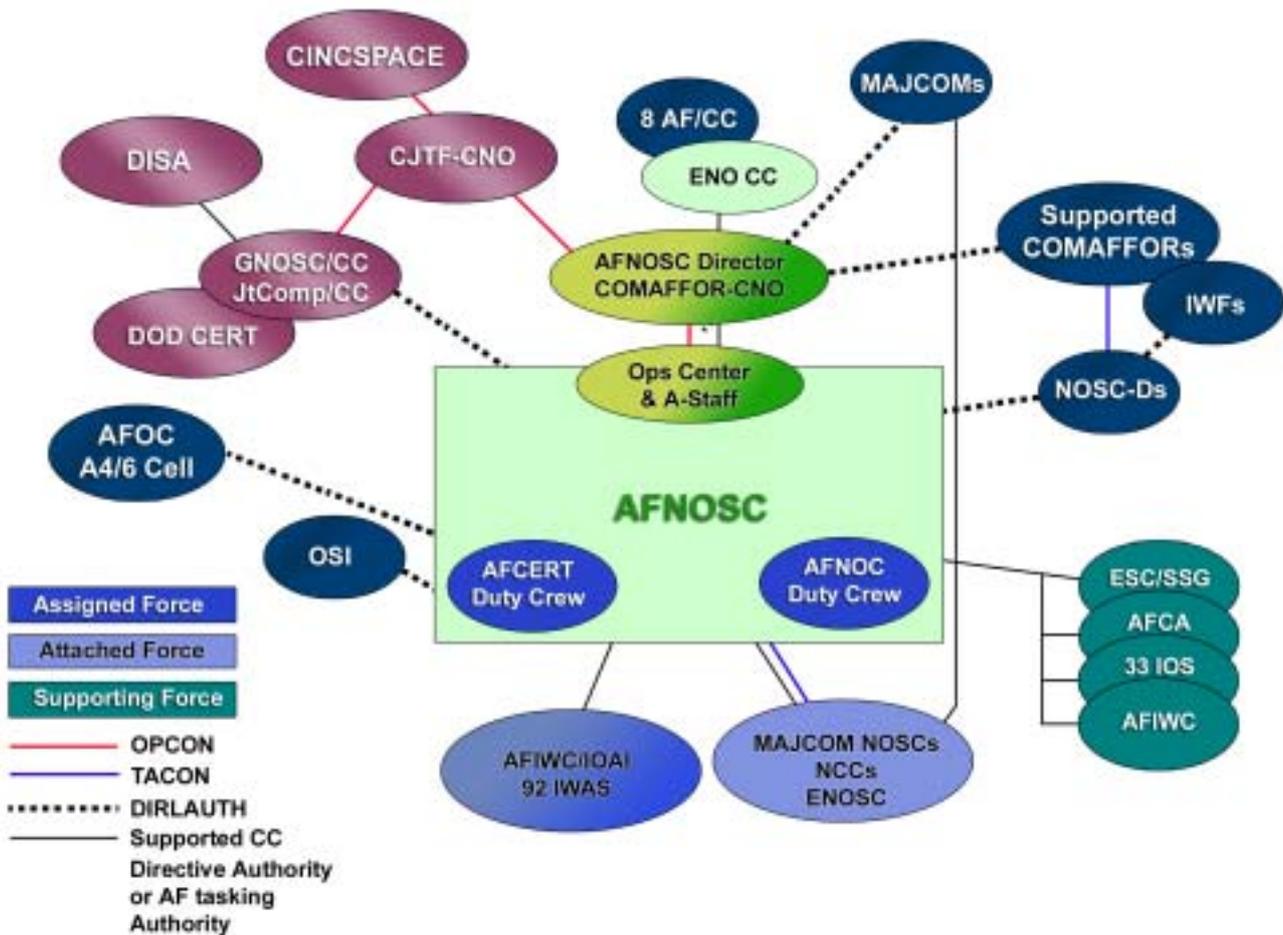


Figure 2

commander of Air Force Forces for Computer Network Operations. The COMAFFOR-CNO Operations Center provides command and control for computer network defense of the Air Force Enterprise, also IA/ENO will be under the authority of the ENO commander to be designated as the 8th Air Force commander. This will bring together both of these functionalities into one centralized location to use the same operations center and create the AFNOSC. The new structure is illustrated in Figure 2.

Eighth Air Force continues to push forward as the AFNOSC proposal awaits approval. The AFNOSC manning began with a small collection of communications officers and enlisted personnel taken from the 8th Air Force's 608th Air Communications Squadron. We recently increased our dedicated personnel from 10 to 18, expanded our operating hours from eight to 14, and increased

our communications capability with the purchase of new equipment. The final proposal calls for a total of about 50 staff members from differing Air Force specialty codes to include a colonel to act as the AFNOSC staff duty officer to provide 24-hour duty crew operations. The state-of-the-art 1,500-square-foot operations center in the new 8th Air Force headquarters building will be modeled after the DOD Computer Emergency Response Team Facility.

The AFNOSC will completely change the way the Air Force handles the command and control of computer network operations. It will enable the Air Force to maintain its information superiority, by giving the Air Force one organization to handle both service-specific and joint computer responsibilities. Please contact us at [commaffor-cno.ops-center@barksdale.af.mil](mailto:commaffor-cno.ops-center@barksdale.af.mil) or DSN 781-1043 for further information about the AFNOSC.



Photo by Tech. Sgt. Paul Cox

Tech. Sgt. Brian Smith works with Master Sgt. Valeria Goehring inside a communications van at a forward-deployed location in support of Operation Southern Watch. Smith, from Robins AFB, Ga., is the lone

active-duty airman working with nine members of the California Air National Guard's 234th Combat Communications Squadron from Hayward ANG Station.

## Comm and info personnel high on request list

**By Lt. Col. Ginger Blazicko**  
*AEF Center Public Affairs and  
AEF Deployment Scheduler  
Langley AFB, Va.*

Who is requested by specialty code to provide their versatile skills and people to communications and information support for U.S. Embassy liaison offices, combatant commanders, joint task forces, headquarters staffs, Homeland Defense offices, Air Expeditionary Wings, and various others? You are correct – communications and information personnel. Comm and info service members are among the approximately 100,000 airmen representing the Total Force – active duty service members, guardsmen, reservists and civilians deployed in support of military operations around the world.

The Air and Space Expeditionary Force, or

AEF, structure is how the Air Force presents fully trained and combat-capable airpower forces to combatant commanders, anywhere and anytime. Since 1999, the Air Force has implemented the AEF as a force presentation tool that embodies one of the key tenets of airpower – flexibility. It allows the Air Force to respond to the full spectrum of military operations, from the humanitarian interventions and exercises through the large-scale major theater contingencies our political and military leaders deem appropriate to achieve our national security objectives.

The AEF can function in two operating environments: steady state and crisis management. Steady state, our normalized battle rhythm which follows a 15-month cycle, typically permits one AEF pair “on call” to handle combatant commander requirements and provides some predictability and



*Photo by Master Sgt. John E. Lasky*

**Senior Airman Patrick (left) and 1st Lt. Bob call in coordinates during an airfield seizure training scenario. Combat weather, pararescue and**

**combat control special tactics school students work together during training exercises. (Image reprinted with permission from Airman)**

stability for our airmen. Usually an AEF will deploy to meet a three-month AEF commitment, followed by a 10-month training period focused on individual skills, exercises and inspections to ensure combat readiness. This ends with a two-month, intensified program heavily focused on forward-deployment preparations. During crisis operations, combatant commanders deal with crisis contingencies and may require resources beyond those available in a single AEF pair. The flexibility of the AEF structure systematically deploys the next, most ready AEF forces, in order, until all the warfighting requirements are filled.

The AEF Center, or AEFC, at Langley AFB, Va., is the Air Force's lead agent for scheduling the most ready and able Air Force forces. The AEFC is the CSAF designated authority for the operational execution of the Air and Space Expeditionary Force construct; including sourcing, scheduling, planning and preparing AEF forces to deploy to global theaters of operation.

The AEFC has a dual-track mission. The flexibility, development, refinement and implementation of the AEF concept are an important part of the mission.

Other key facets of our mission are unit type code, or UTC, restructuring; how we deploy our airmen; use of force modules to support bare-base set-up; and career field manning levels vs. deployable capability.

The day-to-day operational execution of the AEF concept includes sourcing, scheduling, planning and preparing AEF forces to deploy to global theaters of operation. The center accomplishes this through sourcing and scheduling forces in UTCs, deployment guides, Air Force component position descriptions and AEF planning conferences.

Combatant commander requirements are translated by numbered Air Force components into UTCs. Schedulers, representing Air Force specialty codes, work this action to schedule the next, most ready airmen. Using AEF's system tools, such as the Air Force-wide UTC availability system, or AFWUS, often called the library, and the AEF UTC reporting tool, or ART, as well as major command functional area managers.

The Air and Space Expeditionary Support Communications and Information Section, or AESCS,

See LIST Page 35

## ENOSC helps keep systems secure

By **Richard Guidicini**

*Engineer*

*Air Force Communications Agency  
Scott AFB, Ill.*

Ensuring that the Air Force's 750,000 desktop and server computers are kept up-to-date with the latest security patches and operating system enhancements is the mission of the Enterprise Network Operations Support Cell, or ENOSC, at Scott AFB.

The ENOSC was envisioned Oct. 19, 2001, by Lt. Gen. John L. Woodward Jr., now retired, who then served as the Air Force's deputy chief of staff for Communications and Information. He saw a need for a centralized team of software experts who could bring uniform and reliable configuration control to the myriad operating systems used throughout the Air Force's C4I computer system.

The ENOSC became operational when the Technology Directorate of the Air Force Communications Agency, headed by Col. Michael K. McCullough, stood up the patch test bed within one week, and the Web site and help desk two weeks later. Since, the ENOSC has served as the authoritative source for evaluating operating system patches and posting them on the ENOSC Web site. The ENOSC now also manages other Microsoft product patches, such as SQL Server 2000 and Microsoft Office.

At a ceremony marking the first anniversary of the service, McCullough congratulated the ENOSC staff for bringing Woodward's vision to fruition. He said, "Your work is greatly enhancing the security and configuration management of operating systems for the entire Air Force network

enterprise." Susan Ruffcorn, ENOSC's lead engineer, vowed to maintain the pace of improvements by continually refining ENOSC services.

ENOSC personnel resolve compatibility issues before operating system and office automation suite patches are applied. Functional impact testing is performed on the patches to verify their integrity and ensure they will not have any detrimental effects on basic functionality of the operating system. Liaison with private sector operating system vendors is maintained by ENOSC personnel to address Air Force compatibility issues.

ENOSC-approved patches for Windows NT 4.0, Windows 2000, Windows XP, and Solaris 8 operating systems, as well as SQL Server 2000, Microsoft IIS, Microsoft Office 2000 and Office XP, are available 24 hours a day for all Air Force computer configuration management personnel through the ENOSC Web site: <http://www.afca.scott.af.mil/osc>.

In addition to its Web presence, personalized ENOSC support is available by telephone at DSN 779-5244, or e-mail at [enosc@scott.af.mil](mailto:enosc@scott.af.mil) or via the SIPRNet at [enosc@afca.scott.af.smil.mil](mailto:enosc@afca.scott.af.smil.mil). This individualized service provides network operations and security center personnel, and system program managers at the major command and base levels, with direct access to ENOSC personnel. Questions and concerns can be discussed before systems are updated with the latest ENOSC-approved patches.



*Photos by Master Sgt. Ed Ferguson*  
**Steve Miller, AFCA, loads an operating system patch on a network server.**



**Randy Sookoo, AFCA, conducts baseline testing on an operating system security patch.**



Airman 1st Class Jonathan Gordon deployed to Ganci Air Base, Kyrgyzstan out of Holloman AFB, N.M., puts a connector into a hot melt adaptor in an attempt to fix some fiber optic cable.

Photo by Senior Airman Ashley Center

## LIST

From Page 33

has eight schedulers to handle these requirements. These schedulers reflect the total force and include active duty, Guard and Reserve support as well as civilian and government contractors.

AESCS assesses, nominates, and fills communication and information requirements. Requirements for a particular capability may be for a single UTC consisting of one airman, while another UTC may consist of 40 or more airmen based on theater combatant commander needs.

The demand for Air Force specific UTCs is evident in the number of Air Force members deployed supporting the combatant commander requirements. This number changes daily and is available to .mil addresses on the AEF online Web site, <https://aefcenter.acc.af.mil/aefonline/>. The Web site provides links and information on the AEF cycle for the deploying service member.

“Approximately 4,117 communications and information personnel are deployed supporting the global war on terrorism in various locations, as well as providing assistance in humanitarian operations around the globe,” according to Maj. Greta Espeaignnette, Air Force chief of the AESCS section. “Scheduling can be a challenging job. While we deal with codes, numbers and locations, we know there are people, our people, behind them. They have built a solid reputation based on professionalism and abilities. It is no surprise the requirements and kudos for them continue to come in.” Every airman plays an important role in the success of the AEF and the Air Force.



**March 21, 1966:** Air Force Communications Service provided the first communications support for Project Sky Spot in South Vietnam. This was a radar system in which controllers operating mobile radar sets tracked aircraft, corrected their direction and speed, and signalled pilots when they were over their targets.

**March 27, 1973:** The last AFCS unit in South Vietnam, the 1964th Communications Group, moved without personnel and equipment from Tan Son Nhut AB to Ramstein AB, Germany.

**March 13, 1980:** A \$70 million contract was signed with Northern Telecommunications Inc. for the replacement of dial central office equipment with digital telephone switching systems at selected bases. Known as Scope Dial, the modernization project spanned five years.



## Office automation!

Amn. Brian Turbide, operations administration clerk, 2192nd Information Systems Squadron, Loring AFB, Maine, takes a COMSEC test on a new Z-100 computer. The Z-100 was the first system purchased through a small computer requirements contract. Office automation systems changed the way day-to-day business was conducted by automating many functions, such as word processing and records management. (From March 1985 intercom)

## 32nd AOG deploys to support GWOT

Story and photos by Capt. Dani Johnson  
USAFE News Service  
Ramstein AB, Germany

More than 40 airmen from the 32nd Air Operations Group at Ramstein AB left Feb. 2 for the U.S. Central Command area of responsibility to support the global war on terrorism.

The 32nd AOG responded as part of Secretary of Defense Donald Rumsfeld's Dec. 24 deployment order, which directed additional forces to support Operation Enduring Freedom and possible future contingencies.

"We provide command and control for air operations and information operations," said Col. Mace Carpenter, 32nd AOG commander, who was one of the 40 to deploy. "We will take the lead on the strategic planning."

According to Carpenter, the group is the first of more than 170 that will deploy to the U.S. CENTCOM AOR in the near future.

"We are pumped and ready," said Carpenter. "We have been heavily involved in the planning and strategy since April with CENTAF (Central Air Force) at Shaw (AFB, S.C.)."

The mission of the group, which consists of the 32nd Air Intelligence Squadron, 32nd Air Operations Squadron and the 32nd Information Warfare Flight, is to plan, task and direct operational-level air operations by providing intelligence, worldwide deployable communications and air control services.

"We've been preparing our equipment and people for more than three months," said Carpenter. "We have been going through exercises and recalls here, and supporting efforts at numerous locations in the U.S. and here in Europe."

While the group is ready and prepared to deploy, the families have been preparing themselves also.

"It's sad, but we understand why it is happening," said Kelli Bailey, wife of Maj. Pete Bailey, 32nd AIS, and mother to three boys ages 8, 5 and 3. "We'll keep in touch through the Internet, we have a video camera on our computer, and I'll keep our schedule flexible to work with his schedule."



Maj. Anthony Roberson, 32nd Air Operations Squadron, Ramstein AB, hugs his wife, Sheila, daughter Kaley, and son "Deuce" (Anthony II), prior to deploying for the U.S. Central Command area of responsibility.

Karen Carpenter has a slightly different view of the deployment. This is the first time her husband's deployed since she got out of the Air Force. She was a flight surgeon the last time the colonel deployed, but she's since retired.

"This time I don't have a job to keep me occupied," she said. She's staying behind with two sons, 12 and 7, and a daughter, 3. "I'm not in the loop this time, and I'm not worrying as much, since the last two times he was flying (during Operation Desert Storm, the colonel flew the F-111 and in Operation Allied Force flew the F-117 Nighthawk) and this time he is not."

The U.S. Air Forces in Europe Theater Air and Space Operations Support Center commander, Col. Maury Forsyth, was on hand to see the airmen off.

"I wish I were going where you are going," Forsyth said to the troops. "This is serious. It is our chance to show the world why the U.S. is the best in the world."

See story next page

# Florida ANG units active in war on terror

**By Senior Airman Stephen Hudson**  
*Florida National Guard Public Affairs*  
*MacDill AFB, Fla.*

In a back hallway of the 290th Joint Communications Support Squadron hangs a map with a pin in every country where a unit airman has served. The average American probably could not find most of these countries on a map before Sept. 11, 2001. Now countries with names like Afghanistan, Djibouti and Pakistan are the norm.

With their ongoing missions, the men and women of the Florida Air National Guard have proven the term "weekend warrior" no longer applies. Whether it is providing support for homeland defense or the global war on terror, the Florida ANG has found itself entering a new realm – an unexpected one.

The 290th JCSS provides communications to deployed commanders. Before the events of Sept. 11, the unit had prepared for war by participating in exercises around the globe, including Bright Star in Egypt, providing communications in Panama for Air Force Special Operations Command and providing communications during the Florida wildfires of the 1990s.

"I thought the chances of me getting mobilized for a natural disaster were greater than a national security mission," said Senior Airman Jeffrey Strazzere, a satellite wideband maintainer. "Now we are deployed supporting real-world missions." Strazzere, who has been deployed to Afghanistan and the Philippines, said he is thankful for his

employer's support. He had to take a two-year leave of absence from his job at a large communications company.

The 290th JCSS is not the only Florida ANG unit mobilized to support the war on terrorism. The 114th Combat Communications Squadron based at Patrick AFB and the Southeast Air Defense Sector at Tyndall AFB have been engaged in that fight as well. The 114th CCS' satellite communications and its specialized jobs are in high demand around the globe. Thirty-five airmen from the 114th CCS were sent to the U.S. Central Command at MacDill AFB in Tampa. Seven of those later deployed to Qatar to work on the mobile command center for Army Gen. Tommy Franks, CENTCOM commander. Since the terrorist attacks, the Southeast Air Defense Sector's homeland defense mission has grown to include monitoring aircraft flying over land and reacting to airborne threats against population and industrial centers.

"The Southeast Air Defense Sector has two missions," Maj. Todd Breitmann said. "The first is air sovereignty of the United States, and the second is to intercept anyone who enters that airspace. Essentially the two pieces were outward looking prior to 9-11. Since (then), we have to look inward as well." Breitmann, the executive officer at SEADS, added that today SEADS has to work with different agencies to share information, including the Secret Service, the Transportation Security Administration and the FBI. *(Courtesy AFPN)*

Maj. Pete Bailey (left) and Master Sgt. Frank Barker, both from the 32nd Air Intelligence Squadron, Ramstein Air Base, Germany, ensure luggage has proper identification prior to loading onto an aircraft.



*Continued from previous page*

"Don't ever think your job is not important," he added. You all make a difference, every single one of you."

Carpenter spoke to the deploying airmen prior to departing Ramstein.

"We may not be as physically at risk as others," he said. "But we have the burden of the world depending on what you do. Rest assured at the end of the day you will be able to say you've done the best you could, and don't forget to talk and support each other."

The other members of the group tasked to deploy will leave at future dates to more than seven locations throughout Europe and Southwest Asia.

## DOD program helps develop civilian leaders

**By Class of 2003**  
*DOD Executive Leadership  
Development Program*

At “oh-dark-30,” before sunrise, a steady stream of traffic hums past the already bustling Marine Corps Base at Kaneohe Bay, Hawaii. Not an unusual sight for a typical Monday morning – until a couple of nondescript buses abruptly pull off the road and 55 figures clad in black quickly emerge.

While a casual observer might have thought he was witnessing the launch of a clandestine operation, in this case, some of the Marines’ newest “recruits” had just arrived on the scene of their first challenge of the day: Rappel down the 60-foot tower looming ahead of them. Their mission objective: Experience first-hand some of the training, teamwork and mutual trust inherent in preparing to become a Marine.

For these 52 Department of Defense civilians and three active duty military personnel, organized into six teams, Kaneohe Bay was just the first stop in a week jam-packed with orientation visits to all military service branches comprising the Pacific Command theater of operations. This was also the first of 10 one-week deployments for the group over a period of 10 months under DOD’s Executive Leadership Development Program.

ELDP was initiated in the mid-’80s primarily to give some of DOD’s most promising prospective civilian leaders an up-close and personal view of the real-world experiences, training, challenges and issues facing today’s warfighters. In receiving this big picture insight, DOD civilians gain greater awareness, understanding and appreciation of military viewpoints, which in turn helps them develop leadership potential, and become better leaders and decision-makers, as they lead DOD into the 21st century. ELDP applicants undergo an extremely competitive process to enter the program, and must participate in 10 months of physical training and academic coursework in order to “graduate.” About 1,000 civilians have completed ELDP since its inception, with an average of 60 graduates each year.

On that Monday at Kaneohe Bay, the group received a briefing on Marine Forces Pacific com-

mand, as well as instruction in rappelling, and mastering the Marine Corps obstacle course. They shared breakfast at Anderson Dining Hall with young Marines and heard some of their views on retention, quality of life and other issues. That afternoon, they visited Camp H.M. Smith, for briefings on PACOM, and the extensive support provided to the theater by Reserve and National Guard forces.

The busy first day wrapped up with a Pacific Fleet briefing by Rear Adm. Jonathan W. Greenert, COMPACFLT deputy commander, and provided an opportunity for candid dialogue on the command’s unique challenges. A strong proponent of the ELDP course, Greenert said, “I’ve sent two people to your program and it was worth every penny. If your commanders have questions, you can tell them to ask me.”

On Tuesday, the group’s attention was focused on naval shipping, with a briefing and tour of Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility. After a greeting from the facility commander, the class toured two nuclear-powered attack submarines: the USS Los Angeles and USS Pasadena. They learned the historic USS Los Angeles, first of her class, remains among the most effective anti-submarine platforms. They talked with submariners about their experiences and their views on life at sea during often-lengthy deployments away from home and family. It was an eye-opening perspective of the sacrifices of men who stay submerged for months at a time while serving as the silent eyes and ears of our nation’s Naval forces.

Later that day, the group toured Pearl Harbor Naval Shipyard dry docks, where the USS Buffalo was under refurbishment. Escorted by an ELDP graduate, the six teams crawled in and under various sections of the vessel, and observed shipyard workers performing the meticulous, often physically grueling jobs of welding, ship refitting and repairing. They also toured the massive caisson and pump well to see the dry-docking process. The day concluded with a visit to an operating ship fitter and welding shop.

ELDP members spent Wednesday at sea aboard the USS Hopper, the U.S. Navy’s multi-

mission Aegis guided missile destroyer. They saw first-hand the massive teamwork required to bring the sophisticated DDG 70 warship under way.

Under the leadership of Cmdr. Ken Auten, the captain and his crew provided personalized tours of the control room, sonar and radar compartments, berthing areas, mess deck, and the captain's and officers quarters. Affectionately referred to as the "Amazing Grace," the USS Hopper was named after Adm. Grace Hopper, the pioneering female line officer credited with bringing the U.S. Navy into the modern computer age.

Upon disembarking the Hopper in late afternoon, the class took a barge tour of the USS Arizona memorial and "Battleship Row," quietly reflecting on the sacrifices made by the more than 1,500 Navy, Army and Coast Guardsmen who lost their lives on Dec. 7, 1941, in Japan's surprise attack on the world's strongest Navy. The tour gave the group an opportunity to consider that event in the context of today's fight on terror, and their personal experiences during 9-11.

On Thursday, they went to the Army's Schofield Barracks, to observe soldiers of the 2nd Brigade training for the expert infantry badge. ELDP students and staff received hands-on instruction in the techniques employed in range estimation, movement under direct fire, battle emergency medical treatment, rifle training and map reading. After an overview briefing, the brigade's training noncommissioned officers took the six teams through the challenging steps infantrymen must master before earning the highly coveted badge.

Later that morning, the group met with leaders of the U.S. Coast Guard Cutter Kukui, a state-of-the-art buoy tender stationed at Sand Island, Honolulu. The crew conducted various exercises demonstrating the Coast Guard's dual mission as both a law enforcement and a military force. The class received a briefing on the importance of the Coast Guard's unique role in coastal, waterway and environmental protection. The group saw demonstrations of highly skilled pararescue divers performing a search and rescue mission, a simulated law enforcement and interdiction mission at sea, and a buoy tending exercise.

Upon returning to Sand Island, the ELDP members traveled to PACOM headquarters for an intelligence briefing by the Joint Intelligence Command Pacific.

The group spent Friday morning at Special Operations Command Pacific, Camp H.M. Smith,

then returned to Pearl Harbor for a rare opportunity to meet with highly trained Navy SEALs, to hear unclassified accounts of the types of missions they perform, and to see some of the equipment used to carry out covert and special operations.

Later on their last full day at PACOM, ELDP team members received the Pacific Air Forces command brief at Hickam AFB, learning about varied support active and Reserve Component Air Forces provide to the combatant commander, U.S. Pacific Command.

The group ended the day at Joint Task Force Full Accounting with an orientation on how DOD continues to search for prisoner-of-war and missing-in-action personnel to help bring closure for many families who still wait for their loved ones to come home.

The week culminated with a somber yet prideful National Park Service commemoration at Pearl Harbor on the morning of Saturday, Dec. 7. The ELDP students were among hundreds who came to pay respect to the people who lost their lives. The ceremony began promptly at 7:45 a.m., approximately five minutes before the attack began 61 years earlier. Sitting among the few living survivors, it was especially moving to hear the first-hand account of the event's only living Medal of Honor recipient, Chief Aviation Ordnanceman John William Finn. Finn relived his account of the minutes and hours immediately following the attack, painting a vivid picture of chaos, heroism, and the sacrifices of the Navy, Coast Guard and Army men and women who lived and died that day.

"Hearing Finn speak of the tragic events of that day brought to mind the sacrifices and heroism of all the military and civilian personnel who defended our freedom on that day and throughout World War II," said Walt Jones, an ELDP class member. "It also brought to mind those of us who have received the 'baton of freedom' from them and continue their legacy today."

Another ELDP class member, Cheryle Cannady, said, "It was really important that we hear what these WWII vets have to say, especially since many have already passed on, or are getting up in years,"

Like Jones and Cannady, other members of the class of 2003 reflected on the meaning of that day to our nation's history, related it to their own experiences, and resolved to face the challenges of leading DOD into the future.

