

January 2001

*intercom*

**Global Vigilance,  
Reach and Power ...**



**... Information Assurance  
in the 21st Century**

# intercom

Volume 42, No. 1

Headquarters Air Force  
Deputy Chief of Staff for  
Communications and Information  
Lt. Gen. John L. Woodward Jr.

Commander,  
Air Force  
Communications Agency  
Col. Thomas J. Verbeck

## 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 35mm 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/XPPA, *intercom*, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222. Fax is DSN 576-6127 or (618) 256-6127. Editorial staff may be contacted at DSN 576-4396, or (618) 256-4396.

Check out  
our Web site at:

<http://public.afca.scott.af.mil/>



## information assurance



- 5 Sun Tzu concepts guide modern warrior approach to IA
- 6 Networkiness: Roles and Responsibilities
- 8 SSG adds Network Risk Assessment to service portfolio

## in other news

10 Scott member garners  
DOD honors



12 U.S. Transportation Command  
leverages the power of the Internet

14 Scope Warrior XVI  
Comm and Info leaders  
converge on Keesler to plan  
strategies, initiatives, the way ahead



18 JEFX '00 success – workgroup  
managers operationalize information,  
the network

20 Rain, sleet, wind don't deter communications support

22 Recon imagery  
No need to fear unit's arrival

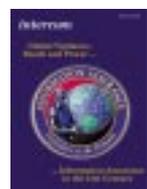
26 Non-stop action helps comm  
group improve deployments



Visit the Computer Based  
Training System Web site at  
<https://afcbt.den.disa.mil>

### About the cover

This month  
marks the start  
of Information  
Assurance  
Awareness  
Campaign  
2001.



Cover by Tech. Sgt. Mike Leonard

# Air Force launches year-long campaign to promote Information Assurance awareness

By Lt. Gen. John L. Woodward Jr.  
*Air Force Deputy Chief of Staff  
for Communications and Information*

Security is everyone's responsibility! Trusted and timely information enables warfighters to leverage the power of information to conduct missions successfully.

Information Assurance provides airmen full-spectrum network protection and availability. The right information, in the right format, to the right place, at the right times – that's Information Assurance.

We must continually remind everyone to guard, protect, defend and observe networks and information content. Networks are definitely maturing – and because they are part of the fight – must also be considered weapon systems!

Emphasizing the importance of IA in all we do, the Air Force is embarking on a year-long Information Assurance Awareness Campaign beginning this month. The theme is "Global Vigilance, Reach and Power: In-

formation Assurance in the 21st Century." The campaign will highlight the responsibilities of the Air Force team to implement sound Information Assurance practices.

I encourage everyone to participate in, and contribute to, the 2001 Information Assurance Awareness Campaign activities, so that we may continue to provide world-class communications and information support to the warfighters worldwide.



**"We must continually remind everyone to guard, protect, defend and observe our networks and information content."**

*Lt. Gen. John L. Woodward Jr.*

## 'Networthiness: Roles and Responsibilities' theme for first month of IA Awareness Campaign

**"Information Assurance is everybody's business in the Air Force – and it's an ongoing responsibility."**

*Col. Thomas J. Verbeck*



By Col. Thomas J. Verbeck  
*Air Force Communications Agency Commander  
Scott AFB, Ill.*

Information Assurance is everybody's business in the Air Force – and it's an ongoing responsibility. Throughout this year, *intercom* will publish a series of articles provided by the major commands and various agencies to help promote Information Assurance awareness. Each month will have a different theme. As focal point for the

campaign, the Air Force Communications Agency is hosting the first month, with the theme "Networthiness: Roles and Responsibilities."

I urge you to read the articles each month thoughtfully, to glean all that you can from them for your personal and professional development, and to offer ideas, suggestions and comments to enhance the effectiveness of IA in the Air Force. Inputs may be sent to [afca-gcis@scott.af.mil](mailto:afca-gcis@scott.af.mil).

Please join me in helping to make this a banner year for promotion of Information Assurance awareness.



## ***Information Assurance Awareness Campaign 2001 Schedule***

<u>Month</u>	<u>Theme</u>	<u>DCS/MAJCOM/FOA</u>
<i>January</i>	<i>Networthiness: Roles and Responsibilities</i>	<i>Air Force Communications Agency</i>
<i>February</i>	<i>Web Security</i>	<i>Air Force/XO and Air Force/SC</i>
<i>March</i>	<i>Digital Devices</i>	<i>Air Mobility Command</i>
<i>April</i>	<i>Threats and Countermeasures</i>	<i>Air Force Office of Special Investigations</i>
<i>May</i>	<i>IA and Deployed AEFs</i>	<i>Air Combat Command</i>
<i>June</i>	<i>User Responsibilities</i>	<i>Air Education &amp; Training Command</i>
<i>July</i>	<i>Communications Security</i>	<i>Air Force Materiel Command &amp; Air Force Special Operations Command</i>
<i>August</i>	<i>Telecommunications</i>	<i>Air Force Reserve Command &amp; Air National Guard</i>
<i>September</i>	<i>IA and Allies</i>	<i>U.S. Air Forces in Europe</i>
<i>October</i>	<i>Computer Network Defense</i>	<i>Air Force Space Command</i>
<i>November</i>	<i>e-mail</i>	<i>Pacific Air Forces</i>
<i>December</i>	<i>IA, The Way Ahead</i>	<i>Air Force Communications Agency</i>

# Sun Tzu concepts guide modern warrior approach to IA

By **David L. Taylor**  
*Information Assurance Policy Branch  
Air Force Deputy Chief of Staff  
for Communications and Information*

The success of our future military operations will depend in part on the quality of our doctrine and policy as well as how grounded we are in the lessons of the past. The legacy of ancient Chinese warrior Sun Tzu includes insightful strategic and tactical combat methodologies that have been studied and successfully implemented worldwide by military leaders for the past 2,500 years. Even as our warfighting technology has continually advanced, especially over the last 100 years, almost all of the concepts articulated by Sun Tzu in his book, *The Art of War*, remain valid for the modern warrior. Sun Tzu's quote, "Anciently the skillful warriors first made themselves invincible and awaited the enemy's moment of vulnerability," clearly aids the shrewd battlefield commander in conducting successful military operations. In addition, Sun Tzu's translated quote above can help us successfully protect our military information systems of today. Here are some specific parallels:

**"Skillful warriors"** should include everyone in our national defense structure and the business of war ... military, civilian and defense contractor. We all have a vital interest and stake in a strong national defense to ensure the preservation of our democratic system of government ... and subsequent leading role in world affairs.

**"Made themselves invincible"** correlates to our dedication to building and maintaining military forces that will succeed in achieving all of our national military objectives. Specifically for our advanced information systems, this requires that we implement a very aggressive Information Assurance program. Our information systems must also be invincible to ensure achievement of our military objectives.

The final part of Sun Tzu's quote, **"and awaited the enemy's moment of vulnerability,"** means that in building our powerful forces, we must never turn our attention away from the efforts and strategies of our

potential adversaries. In regard to IA, we have been continually engaged with numerous foreign and domestic enemies for several years. Hackers, crackers and other assorted criminals have become a serious threat to our national military information systems. Fortunately, our current and future IA initiatives will continue to minimize this threat. In addition to effective initiatives, we must constantly look at our programs and ensure everyone keeps a vigilant IA mindset when operating our information systems. Studying Sun Tzu and other experts can help us keep our focus and perspective regarding our objectives. We must also do much more to ensure our continued invincibility.

As the Information Assurance Awareness Campaign kicks off this month, we urge you to actively participate and do all you can to ensure this campaign is highly successful. Prior to 2001, the Air Force set aside one month each year to focus on IA awareness issues and activities. However, the rapid proliferation of information system and network utilization and the increasing threats to these systems have made it imperative that we promote an aggressive

awareness campaign on a continual, year-round basis. As the campaign progresses, we look forward to your contributions and feedback, which may be sent to [david.taylor@pentagon.af.mil](mailto:david.taylor@pentagon.af.mil).

On a monthly basis, IA information will be presented by the Deputy Chief of Staff for Air and Space Operations, Secretary of the Air Force Inspector General, as well as Air Force major commands and a few Air Force Field Operating Agencies within their respective core expertise areas. This is a superb opportunity for Air Force members to gain operational insight into this vital mission area. Additionally, IA promotional items will be provided to remind personnel of computer and information security requirements. Finally, about 500 newly minted IA medallions will be awarded to our top IA contributors throughout the Air Force during 2001. Our ultimate goal is to keep IA foremost on the minds of every Air Force member and minimize the potential of system compromise or exploitation. We can't afford a single **"moment of vulnerability."**

(Mr. Taylor is a research analyst, Analytic Services, Inc.)

***"Anciently the skillful  
warriors first made  
themselves invincible  
and awaited  
the enemy's moment  
of vulnerability"***

***Sun Tzu***



# Networthiness: Roles and Responsibilities



By **Cynthia M. Crowe**  
*Air Force Communications Agency*  
*Scott AFB, Ill.*

Do you know what your responsibilities are and what additional roles you may be performing in today's network-centric environment? It's important to know what's expected of you.

A good starting point is AFI 33-202, *Computer Security*, which defines some key roles, such as the Designated Approving Authority, Certifying Official, Computer Systems Security Officer, and the user. How many times have you heard some of these terms, without fully understanding what they are, or their associated roles?

As a computer user, do you know your responsibilities? It's the simple things like constructing a good password and protecting it; virus scanning all magnetic media (fixed and removable); following security policies established for the network; and reporting system security incidents, vulnerabilities and virus attacks to your local Computer Systems Security Officer.

The CSSO is the first person to contact for assistance when questions arise about the security of your system, if a virus is detected, or if a vulnerability is identified. The CSSO ensures users comply on a day-to-day basis with local network and system security policy. Another important part of the CSSO duties is

to maintain the Systems Security Authorization Agreement for all systems under their control. Workgroup Managers may perform some or all of the duties of the CSSO.

Before loading any software onto your system, you need to identify your software requirement to your WM.

Software may be loaded onto a government computer with the approval of the DAA, in coordination with the Network Control Center.

The DAA has overall responsibility for secure operation of the information system. He or she makes the appropriate decision to balance security requirements, mission and resources against a defined or perceived threat. DAAs must have the resources to expend in support of certification and security countermeasures.

The Certifying Official is appointed by the DAA to assist with the certification and accreditation process. The CO makes technical judgments regard-

ing an information system's compliance with systems security policy, and develops an accreditation recommendation for submission to the DAA. If the information system is a complex or large network, the CO forms and leads a certification team.

There are numerous other roles at the wing and MAJCOM levels. It's important to know your roles and responsibilities and who to contact the next time problems arise. Your wing Information Assurance Office can provide additional clarification.

## Key Terms

### **Computer Systems Security Officer-**

First person to contact for assistance when questions arise about the security of your system, if a virus is detected, or if a vulnerability is identified. Maintains the Systems Security Authorization Agreement on all systems under their control.

### **Workgroup Manager-**

May perform some or all of the duties of the CSSO. Check with the WM before loading any software on your computer.

### **Designated Approving Authority-**

Has overall responsibility for the secure operation of the information system.

### **Certifying Official -**

Makes technical judgments regarding an information system's compliance with the systems security policy, and develops an accreditation recommendation for submission to the DAA.

# Process identifies risks, protects AF networks

## Certification and Accreditation

By Master Sgt. Paul Gorom  
Air Force Communications Agency  
Scott AFB, Ill.

These words can strike fear into a wing's Information Assurance office, network control center, and program management office. If a C&A is accomplished, everyone can breathe easy. If one is not done, it could later require months of painstaking research into every aspect of a system, network and stand-alone PC. Almost every type of comm inspection (such as a Major Command Information Protection Assessment and Assistance Program, or an IG Special Interest Item for Information Assurance) asks if all networks and systems on your installation are certified by the appointed certifying official and accredited by the designated approving authority.

Why the emphasis on C&A? Many public laws and DOD or Air Force Instructions mandate the process, but the question is still "why"? A proper C&A identifies everything the DAA, certifying official, and functional manager

will ever need to know about that system. A C&A identifies all threats and vulnerabilities (risks) associated with the system, including all functional systems and networks. It details the actions taken to mitigate risks to an acceptable level (residual risk). It also lays out the functionality, performance issues and budget for the life cycle of the system. The bottom line is, a C&A tells the DAA what residual risk is associated with the system and its potential to impact the Air Force network infrastructure.

Notice I didn't say the base network infrastructure, but the Air Force network infrastructure. We are at the point where one base network infrastructure can affect all bases. If 99 percent of all Air Force bases are certified and accredited and all known vulnerabilities are mitigated, that last one percent which has not identified and corrected their vulnerabilities, could be the open door the bad guys (hackers) exploit to gain access to our networks. The bad guys can then use that door as a jumping point to other bases and networks.

In our Air Force publications, we state the PMOs are responsible for C&A, but we haven't been diligent

in enforcing that requirement. We have allowed systems to be installed on our bases, connected them to the network, and then expected the base to do the C&A. Two problems come to mind. First, having every base accomplish its own C&A is redundant. Second, most bases don't have the technical expertise with every system to do a proper C&A. In many cases, only after a system is operational, are the vulnerabilities associated with that system identified and brought to the attention of the DAA. But as we all know, once a system is connected and in use, it's very difficult to disconnect the system, due to mission requirements.

So what is the Air Force doing to prevent this from occurring in the future? We are enforcing the Command, Control, Communications, Computers and Intelligence Support Plan requirement mandated by DOD regulation 5000.2-R. The purpose of the C4ISP is to identify requirements necessary to ensure a system under development will be fully supportable once handed over to the operating community. The Air Force flavor

of the C4ISP looks at system-to-system interoperability, intelligence support, Joint Technical Architecture – Air Force compliance, security and networkiness. To make networkiness a reality, the Air Force has initiated the Certificate of Networkiness.

The Certificate of Networkiness process describes the relative risks associated with fielding a networked system or application. A networky system can be sustained from a comm and info perspective and any risks that it may present are deemed to be acceptable. Part of the Certificate of Networkiness process is to review the C&A effort.

To add integrity and to prevent this process from becoming just another paper shuffle, the Air Force Chief Information Office signs the Certificate of Networkiness, stating the system has been evaluated and doesn't pose an unacceptable risk, in terms of networkiness, to the Air Force Enterprise Network. If a system is not "networky", the AF CIO will not issue a Certificate of Networkiness. Alternatively, the CIO might issue a Certificate of Networkiness with conditions.

A condition may place limits on the operation of the system (such as only behind the firewall or on its own server) or identify actions that must be accomplished within a specified time period (such as provid-

**If 99 percent of all Air Force bases are certified and accredited and all known vulnerabilities are mitigated, that last one percent which has not identified and corrected their vulnerabilities, could be the open door the bad guys (hackers) exploit to gain access to our networks.**

See C&A Page 27

# SSG adds Network Risk Assessment to service portfolio

By Senior Master Sgt.  
Sue Garland  
Standard Systems Group  
Software Factory  
Maxwell AFB-  
Gunter Annex, Ala.

The Air Force Communications Agency has licensed the Standard Systems Group Communications Environment Test Lab, to provide network risk assessments for automated information systems intending to use Air Force networks, moving the Air Force closer toward its Information Assurance objectives.

SSG designed the CETL to emulate a network control center environment, using standard Air Force communications infrastructure management hardware and software. Seven team members provide system administration for the \$2 million network facility, as well as testing support to more than 50 automated information systems.

The CETL was authorized by Dr. Lawrence Delaney, Assistant Secretary of the Air Force for Acquisition and Chief Information Officer, to perform network risk assessments as part of the Certificate of Networkworthiness process. The assessments include analyzing each system for impact on the network, interoperability with the infrastructure, and network security. Security testing focuses on password security, logins and port scans, impact on network bandwidth, and compatibility with communications and information infrastructure, including base network infrastructure. Test results, along with system certification and accreditation packages, provide major commands the documentation and evaluation necessary to load systems on the base level infrastructure.

"The Air Force has acquired or fielded systems in the past that presented network security vulnerabilities, wouldn't work with typical base infrastructure, or lacked worldwide access, and others that were simply underfunded for sustainment," said Master Sgt. Amanda Bowman, Network Test Branch superintendent. The result, she said, was program delays, increased costs, and network vulnerabilities.

"Licensing SSG to perform this work further seals the partnering relationship between SSG and the rest of the Air Force to improve networkworthiness," said Robert Frye, SSG executive director. The SSG test lab joins



Photo by Bud Hancock

**Test lab technicians Senior Airman Barry Franklin and Mr. George Helms ensure Local Area Network connectivity for Standard Systems Group's Software Factory testers.**

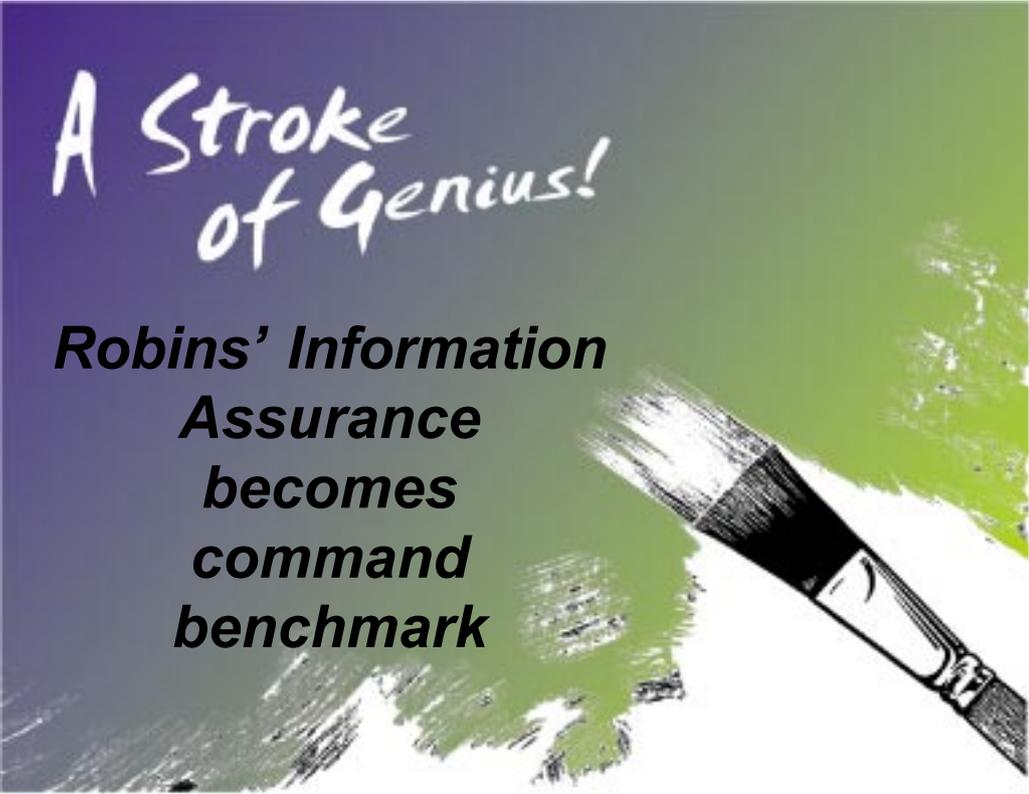
the Air Force Network Test Center at Scott AFB as the only facility licensed to test for Certificate of Networkworthiness. While the CETL is concentrating on SSG's systems now, it can extend the service to other agencies, Mr. Frye added.

The concept of Certificate of Networkworthiness was first envisioned by Lt. Gen. William J. Donahue, former director of Air Force Communications and Information, who got the nod from Dr. Delaney to stand up the first Air Force network test center. "This is a disciplined process for success that attacks current disconnects and establishes effective and efficient measurable processes," Dr. Delaney said.

The networkworthiness process ensures systems are only fielded when they're sustainable, standards compliant, and impose minimal risk to Air Force networks and other systems. Any deviation from the Air Force instructions will require waivers to operate.

The CETL, part of an independent test organization at SSG, has completed several network risk assessments to date, including the Modernized Supply System, Defense Message System-Air Force, and the Standard Procurement System. Normal target time for the network risk assessment process is 30 days, which should decrease as this process is further refined.

For more information, visit the CETL Web site at <http://www.ssg.gunter.af.mil/softwarefactory>.



*A Stroke  
of Genius!*

## **Robins' Information Assurance becomes command benchmark**

**By Chris Zdrakas**  
*78th Air Base Wing  
Robins AFB, Ga.*

Headquarters Air Force Materiel Command took one look at the 78th Communications Squadron's Information Assurance practices and liked what it saw. Now Robins AFB's practices are about to become the command's benchmark.

Headquarters invited Master Sgt. Lesley Lirley, manager of Robins' Information Assurance operations, and Staff Sgt. Anthony Knoll, the squadron's information technology authority, to Wright-Patterson AFB, Ohio, to tell their success story to headquarters personnel.

The invitation stemmed from a briefing the Robins Information Assurance team presented to Debra Haley, director of Headquarters' Communications and Information. Ms. Haley, who was at Robins for a change of command ceremony, had requested the briefing because of Robins' success in the recent Unit Compliance Inspection. But her direction came from the top—Gen. Lester L. Lyles, who Sergeant Lirley said “wanted to see what we're doing right.

“The briefing gave headquarters a front-line view of Information Assurance—a view from the trenches,” Sergeant Lirley said. “It seemed to open their eyes to something new. Headquarters had been approaching all aspects of Information Assurance from the individual's standpoint—program to program individually. We view Information Assurance as an all-inclusive process.”

Headquarters' specific interest was in Robins' certification and accreditation status in the command, and a new emphasis on Information Assurance known as “operationalization.”

“We met with headquarters' Information Assurance people and hammered out a plan to help accredit all computers in AFMC by the end of August,” Sergeant Lirley said. He and Sergeant Knoll demonstrated how AFMC could use a Robins-developed database, which Sergeant Lirley said is “the heartbeat of our Information Assurance operations.

“It allows us to track every piece of equipment on base, issues AFCERT (Air Force Computer

Emergency Response Team) computer security advisories, collects status on completing patches and provides online certification, among other services,” Sergeant Lirley said. The system provides client versions of the database to allow computer security teams at Robins to see system information in real time. The Communications Squadron's Information Assurance team can see real-time data on certifications and updates to the base's more than 20,000 systems in the database.

“Our information is constantly changing, and the database allows us to make certification and accreditation a living document,” Sergeant Lirley said. “The grassroots efforts of our computer security partners at the organizational level to keep data current is the key to the program's success.”

Headquarters also wanted to know more about Robins' computer virus wall, the barrier that keeps out viruses, nuisance e-mail and “spam” mail. Three other bases have implemented similar electronic barriers, he said.

“I would say the bottom line is that headquarters saw a process at Robins that it didn't see in the rest of the command, and it wanted to implement our policies, procedures and lessons learned throughout the command. This is a major step in the right direction because headquarters is looking at life from the warfighter's view on the front lines.” Sergeant Lirley added that his organization does virtual battle on a daily basis as information-hungry countries all over the globe, and virus creators bent on seeing how far their destructive viruses will go, continue to attack Air Force systems.

# Scott member garners DOD honors



**Susan Kunz works with Airman 1st Class Andrew Lepperd in the Air Mobility Command television productions and video editing suite.**

**Story and photos by Bob Fehringer**  
*375th Airlift Wing Public Affairs Office*  
*Scott AFB, Ill.*

Susan Kunz, assistant base visual information manager, traveled to the Pentagon in October to receive her award as Department of Defense Outstanding Employee with a Disability for 2000.

Recently the Pentagon came to Ms. Kunz in the form of Deputy Chief of Staff for Personnel Lt. Gen. Donald Peterson.

General Peterson stopped by the visual information flight to present Ms. Kunz his department's coin and personal words of congratulations.

Ms. Kunz, paralyzed at age 13 during surgery to remove a tumor from her spine, has been an award-winning Air Force illustrator and manager for more than 22 years.

"She has the information, she has the knowledge," said Capt. Mark Horony, visual information flight commander. "She takes care of this flight. She's kept us above ground."

Ms. Kunz is modest about her accomplishment and the resulting award.

"I did my job every day," she said. "I came to work every day. It's kind of the nature of the job. You feel like you're doing something important and it's part of something else that's big and important in the defense of your country."

Ms. Kunz remains optimistic about her work within the Air Force community.

"There's always something different," she said. "You never know what kind of requirement is going to come through the door. I enjoy the mix of people. We have

civilians who I've worked with for years, but then there's always somebody new with the military.

"I have the best job in the Air Force," Ms. Kunz added. "I get to do what I enjoy and it's for a good purpose."



**Lt. Gen. Donald Peterson, Air Force Deputy Chief of Staff for Personnel, presents Susan Kunz with his department's coin and personal words of congratulations for being named DOD's Outstanding Employee with a Disability for 2000.**

# Air Force Communications Agency fields Network Training Centers

*Twenty-one centers  
established for computer  
network training*

**By Senior Master Sgt. Ted Crincoli**  
*Air Force Communications Agency  
Chief, OPTN Plans and Implementation  
Scott AFB, Ill.*

Having the right information anytime and anywhere in the world is essential for decision-makers and commanders. Lack of training in skills necessary to do network operator functions—both today and in the future -- is a problem in the Air Force that affects the entire communications and information community. Raising the knowledge level of computer networking to all 40,000 plus members of the comm and info community is the goal of a newly fielded initiative called structured on-the-job training. SOJT, a program under Operationalizing and Professionalizing the Network, is a classroom filled with the latest hardware, software, curriculum, and a qualified instructor to teach these “must have” skills.

The Air Force Communications Agency has partnered with Cisco and Science Applications International Corporation to field Network Training Centers at the first 21 locations. The ultimate goal is to field the centers at every base with a comm and info population of 100 or more. This partnership will facilitate standardized computer networking training across the Air Force. The skills to be taught range from basic computer hardware and software foundational training, to designing, building and maintaining complex computer networks. This training provides a strong foundation for future computer training and builds on initial skills taught at Keesler AFB, Miss. Instruction is started in a curriculum provided by Cisco called the Cisco Network Academy, which provides basics of networking along with additional semesters of instruction in Routers, Switches and Wide Area Networks. The classes integrate more than 280 hours of computer-based training, instructor lecture, and hands-on demonstrations and tests.

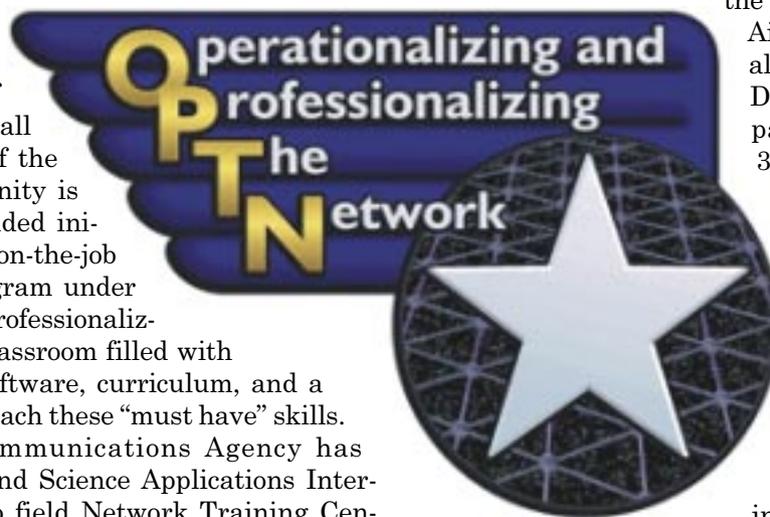
In these times of drawn-down forces, increased operations around the world and doing more with less, on-the-job training has suffered severely. Commanders have said with “experienced” manning levels down, the ability of work centers to send someone off to one of the advanced skills courses for school is difficult. By placing a classroom and instructor at each base and having an in-depth curriculum designed to be taught over a number of months, TDY time is reduced, and trainees receive instruction at a pace that facilitates maximum retention.

In the future, computer skills all comm and info professionals require will continue to grow, as technology becomes more and more complicated. That's why the first semester of the Cisco curriculum, Introduction to Networking, is recommended for everyone in

the 3A, 3C, 3V, 2E and 33S Air Force Specialty Codes, along with Department of Defense civilians in Occupational Codes 301, 318, 326, 332, 334, 335 and 391. In addition, anyone else whose supervisor and commander feel the Air Force would benefit from the training are encouraged to attend. The goal is to take the knowledge of all members of the comm and info community to a higher level.

Implementation of the program is the responsibility of the Air Force Communications Agency. AFCA purchases equipment, contracts instructors, and provides policy and guidance for the program. Bases are responsible for managing project implementation at local level. An individual is assigned at each base to act as liaison with the contracted instructor and to identify training needs. Together they create a course schedule that addresses those needs and schedule students for the classes. This can be solely the Cisco Academy curriculum, Windows NT, Exchange 5.5, Workgroup Management or any combination.

For more information on the structured OJT program visit the AFCA OPTN Web site at <http://www.afca.scott.af.mil/optn>, or contact the office at DSN 576-2798, e-mail [afca-gclo@scott.af.mil](mailto:afca-gclo@scott.af.mil).



# U.S. Transportation Command leverages the power of the Internet

By Dave Patterson

*U.S. Transportation Command Public Affairs  
Scott AFB, Ill.*

U.S. Transportation Command has long recognized that information is the key to success in any global endeavor. This recognition is reflected in efforts to leverage e-business concepts and tools to “DOT COM” the Defense Transportation System.

“Through the power of the Internet we intend to bring together our customers, business partners, suppliers and employees to meet the transportation needs of the Department of Defense,” said Brig. Gen. Gilbert R. Hawk, director of Command, Control, Communica-

tions and Computer Systems, J6. “Our ability to access and use information makes USTRANSCOM the best in the business.”

At this time, J6 is shifting away from an application-centric approach to providing capabilities-centric information tools. The information management team is developing processes, standards and tools to manage data as a corporate asset. J6’s goal is to improve the quality of DTS data by eliminating data redundancy and providing access to the originating source—the data truth. To reach this goal it must be provided accurately, consistently, completely and in a timely manner. To help visualize information, J6 is also building standard tool sets that allow the user to bring together fused in-



The U.S. Transportation Command Business to Employee Portal will be a customizable Web view to access visualization tools for

decision ready information, legacy applications, electronic mail and administrative tools.

formation to facilitate quality decision-making.

“Our target with the use of Internet technology is to provide the right information to the right users at the right time,” General Hawk said. “To meet our needs for fused information to facilitate decision-making, we must be able to access information anywhere in the world, from the foxhole to the safety of our own homes. The tools we are developing will someday allow the user to access the DTS data warehouse through a single entry point called a ‘portal.’ Based on a user’s role in the transportation community, he or she will be able to access a portal, ask a question, and receive the information in a form that will facilitate making good decisions.”

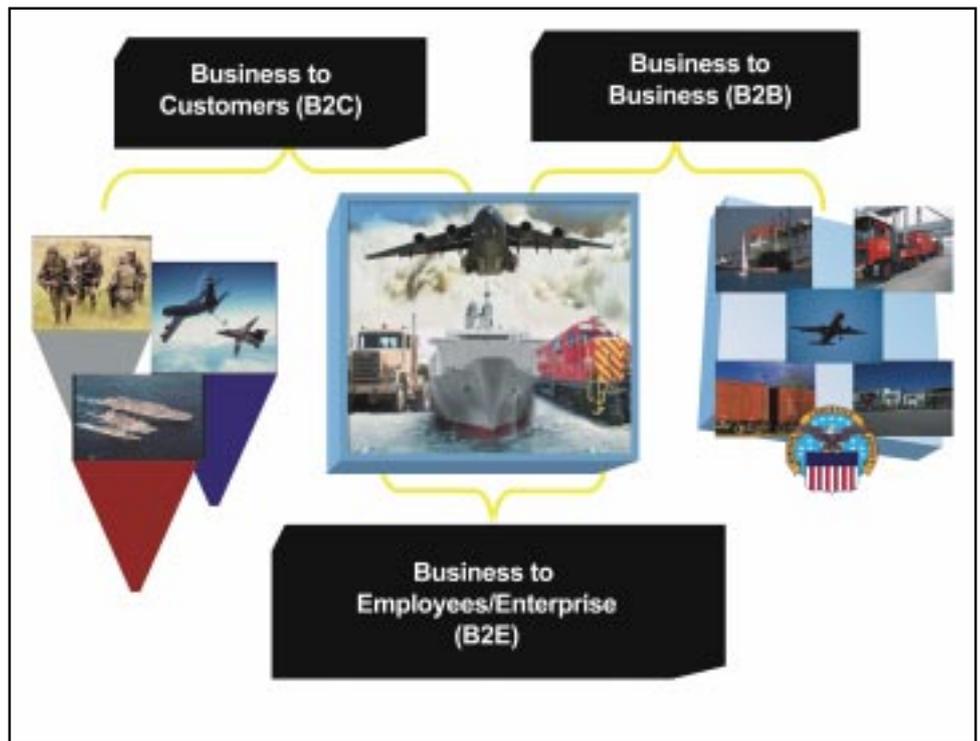
The J6’s Programs Division has embarked on their first efforts toward these goals—the Local Area Network Enhancement Initiative.

“This initiative is a two phase effort,” said Lt. Col. Stephen James, chief of the division. “We’re making improvements to our current network, and setting a foundation that we think will be an important step to eventually get the headquarters into what people in industry are calling e-commerce or electronic business, which will take some time. The funding for the ‘e-biz’ phase will not be available until FY ‘02.”

According to Gail VanWinkle, chief of the division’s Business Systems Branch, “A big part of the LAN Enhancement Initiative is the public Web page and the business page. We’re trying to make them more logical and expand their capabilities—to have more tools and useful items out there for the general USTRANSCOM population and customers of the command.”

“A lot of people will give you the wrong definition of electronic business,” Colonel James said. “In our view, electronic business is more than just transforming our requirements for IT and putting them onto the Web. We must allow users access to DTS data, both structured and unstructured, from a corporate view, while capitalizing on Internet technology. Today you may have to log onto three or four systems to find information—this will eliminate that level of complexity. This will not be an easy task but we’ve already made incremental progress. With some continued success, I think everyone will soon have a better understanding of electronic business.

“I think there’s another idea that helps to understand all this,” Colonel James said. “You could consider where we are right now with our office automa-



**U.S. Transportation Command portals will focus on several user groups based on their information needs.**

tion systems at USTRANSCOM. Having workstations on every action officer’s desk brought us to the end of the first generation, where we are all connected together and can exchange certain information in the form of e-mail and files. But for most people today, when they come into their office and turn their computer on, the first thing they see is a collection of icons scattered all over their display. When you select one of these icons, it starts an application such as Outlook e-mail. We’ve gotten to that point in an unstructured way. It’s not been integrated in any shape or form.”

“If we continue down the path of not trying to organize the growth on the network,” Colonel James said, “you can envision a time in the future when we come in to work and find 50 or more application icons on our display that require a different password and logon name for the user to remember. The use of the Internet, portals and Web-based applications will obviate the need for the multitude of applications resident on your workstation.”

“Harnessing the power of the Internet will extend the availability and accessibility of transportation information,” General Hawk said. “We are building on the successes and lessons learned of industry to create a robust DTS. Only when we have the ability to move information seamlessly can we expect operators to efficiently evaluate our ability to supply deployed forces in a cost-effective and timely manner. Seamless information will enable us to globally schedule, track assets and provide accurate in-transit visibility to decision-makers. We need to know exactly where our people and cargo reside 24 hours a day, seven days a week.”

# Scope Warrior XVI



Above: Lt. Gen. John L. Woodward Jr., kicks off the conference. The Air Force Deputy Chief of Staff for Communications and Information co-hosted the conference with the 81st Training Wing at Keesler. Right: Brig. Gen. Roosevelt Mercer Jr., 81st TRW commander, welcomes Scope Warrior XVI attendees.



**Left: John M. Gilligan makes a point with Brig. Gen. Anthony Bell Jr., director C4 Systems, U.S. Joint Forces Command J6. Mr. Gilligan is the new AF co-deputy CIO, a position he shares with General Woodward.**

## Comm & Info leaders converge on Keesler to plan strategies, initiatives, the way ahead

**KEESLER AFB, Miss.** — Senior communications and information leaders met Dec. 4-7 at Keesler AFB, Miss., for Scope Warrior. The annual worldwide conference provides the Air Force comm and info warfighter community a forum to discuss policies, direction, strategies and current and future initiatives.

Scope Warrior XVI's theme was "One Air Force ... One Network." It is also the strategy for changing how the Air Force leverages information technology to improve combat effectiveness and daily mission performance.

"This conference is an opportunity to lay current issues on the table as well as the issues of tomorrow," said Lt. Gen. John L. Woodward Jr., Air Force Deputy Chief of Staff for Communications and Information. "It's about shaping, responding, and most importantly, proactively engaging. The whole idea is to think strategically, talk to each other, exchange information, and lay the framework for solving the network challenges for our Air Force," he added.

This year's conference was formatted to include six strategic discussion sessions designed to quickly get issues on the table and establish courses of action.

General Woodward challenged participants to use the conference's structure to help map the way ahead for increasing combat power for every airman.

Briefings to set the stage for strategic discussions were presented by each major command SC, Air Force comm and info general officers, and other special distinguished guests including the directors from Defense Information Systems Agency and Electronic Systems Center, both deputy Air Force Chief Information Officers, Joint Task Force J6s from Southwest Asia and Korea, and the comm and info and comm-electronics enlisted career field functional managers. Subjects included Aerospace Expeditionary Force; what comm and info brings to the fight; network-centric operations; partnerships; people; and resourcing.

Points of emphasis included ensuring all AEF associated comm and info people can link themselves and their jobs to their appointed AEF and deployment calendar. Participants placed great importance on expanding comm and info-wide understanding of core compe-

See **SCOPE WARRIOR** Page 16

## SCOPE WARRIOR

From Page 15

tencies, such as satellite communications and data linking.

Within network-centric operations discussions, the group endorsed ongoing IT Summit initiatives and emphasized the need for standardized levels of desktop PC services and applications, and continued support for treating the network as a weapon system.

Lt. Gen. Leslie Kenne, the commander of ESC, opened the session on partnerships and emphasized the importance of partnering. The newest Deputy Air Force CIO, Mr. John Gilligan, Principal Deputy Assistant Secretary for Business and Information Management working for AF CIO, Dr. Lawrence Delaney, brought a wealth of knowledge and experience to discussions on key partnerships. Lt. Gen. Harry D. Raduege Jr., the Director of DISA, described his organization's philosophy and commitments to service. USTRANSCOM and AFRC senior comm and info leaders also presented introductory messages. Discussion highlights included the need for continued emphasis on information assurance and service level agreements, the relationship of C4 systems integrated support plans to the acquisition process, and CIO strategies, standards, and processes.

Leaders from the Air Force SC staff, the Developing Aerospace Leaders staff, military and civilian rep-



**Lt. Gen. John L. Woodward Jr., talks about comm during the Korean War with Dr. Tom Snyder, Air Force comm and info historian from AFCA.**

resentatives from Air Force Personnel Center, the Air Force Frequency Management Agency, career field functional managers, and training schools opened the people-centered discussions. Among topics for follow-up were continued emphasis on training, career long professional development, and incentives.

Rounding out the hectic two-day sessions, Air Force Materiel Command, DISA, and Air Education and Training Command leaders set the stage for resourcing discussions leading to clarification of DISA pricing strategies, exploration of cost performance models for measuring network services, and a call for standardized desktop computer service levels.

The local Armed Forces Communications and Electronics Association chapter held a luncheon in conjunction with Scope Warrior. The highlight of the conference was a dining-in, held on the final night of Scope Warrior with special guest speaker, Maj. Gen. Leroy Barnidge Jr., vice commander, 9th Air Force, and deputy commander, U.S. Central Command Air Forces, Shaw Air Force Base, S.C., who described the decisive combat edge global "comms" delivered to members of his B-2 command as they helped fight and win the air war over Kosovo.

Also during the Scope Warrior Dining In, Capt. Raymond Powell of the Air Force Pentagon Communications Agency won the Lt. Gen. Lee Paschall Award and Capt. Hope Cullen of the 355th Communications Squadron won the Maj. Gen. Robert Sadler Award for the top ACOT/BCOT students (respectively) of the year.

The conference hosts, the 333rd Training Squadron and 81st Training Wing at Keesler AFB, made it all possible and with their superb support, earned high praise and many thanks from all conference attendees.



**Maj. Jodine Tooke and David Hangsleben, HQ USAF/SC's Director's Action Group, go over Scope Warrior XVI details with Lt. Gen. John L. Woodward Jr.**



**Top left: Lt. Gen. Harry D. Raduege Jr., Director of DISA, and Brig. Gen. Gil Hawk, USTRANSCOM J6, talk during a break at Scope Warrior XVI.**

**Top right: Lt. Gen. John L. Woodward Jr., and Colonel Steve Woolf look at a display that honors comm and info pioneers.**

**Above: General Woodward makes a point during the conference.**

**Left: Lt. Gen. John L. Woodward Jr., presents Capt. Raymond Powell with the Lt. Gen. Lee Paschall Award as top student in ACOT.**

# JEFX '00 success – workgroup managers operationalize information, the network

By Chief Master Sgt. Elaine LaMaster  
*Air Combat Command  
Langley AFB, Va.*

Joint Expeditionary Force Experiment 2000 is an Air Force Chief of Staff-sponsored experiment combining live-fly forces, live-play ground forces, simulations, and technology insertions in a joint/combined warfighting environment. JEFX is extremely ambitious where new and emerging technologies to fight future wars are tested to solve real-world warfighting conditions. JEFX '00 involved more than 3,000 participants at 11 strategic sites across the nation, examining 45 leading-edge process and technology initiatives to enhance the 21st century Expeditionary Aerospace Force.

As evidenced by the 385,000 hits on the Web page and 91 percent satisfaction rating from warfighter feedback, workgroup managers improved Combined Forces Air Component Commander information awareness, access, and delivery management. Their efforts streamlined processes and enabled faster, better decision-making, thus significantly enhancing aerospace operations. In order to ensure "repeat performance," WMs docu-

mented more than 100 operational procedures and checklists for managing information. They were directly responsible for the unprecedented success of the Air Force Chief of Staff's \$64 million experiment. The Combined Air Operations Center singled out WM efforts as one of the great successes of JEFX '00.

The CAOC at Hurlburt Field, Fla., the Air Operations Center at Nellis AFB, Nev., and the Operations Support Center at Langley AFB, Va., controlled the JEFX '00 command nodes and relied on our workgroup managers to ensure operations centers had immediate uninterrupted access to network systems. To test the initiatives and support the air operations 250-plus sorties, the sites were linked together by a robust voice, video, and data network handling gigabit information flows from satellites to the network and between sites. Air Force information managers more than earned their money in this fast-paced, high-stress environment. They proved the value of their information and workgroup management skills in ensuring operational availability of information and the network. These information managers enabled the Aerospace Component to more effectively support the Joint Forces Commander.

The experiment's complex networking environment made the WMs' goal to manage and improve access, control, flow of information and collaboration of command and control information systems extremely difficult. They and many of the operators had no previous experience with Theater Battle Management Core System and a baseline didn't exist for user profiles needed within TBMCS. This presented new challenges for the WMs, who had to develop and implement new procedures to manage the information content and operational flow and presentation in a dynamic high ops environment.

To learn TBMCS user administration and basic troubleshooting, the WMs worked closely with the Network Control Center and the TBMCS Program Office to set up Unix and NT workstations and create and maintain user ac-



**Tech. Sgt. Terrance Meyers, Senior Airman Charles Powell, and Chief Master Sgt. Elaine LaMaster (the functional IM team) build and manage the intranet providing information management services to the AOC.**



**Tech. Sgt. Lorenzo Thomas shows Senior Airman Eugene Magana (ISR division workgroup managers) how to use the workflow, document, and records management application to facilitate information flow based on commander's policies.**

counts. More than 10,000 jobs were worked to support 1,200 operators on the network during JEFX '00. Once WMs had the proper administrative permissions to assist network users, they were able to greatly reduce workload on the Help Desk, Information Workspace, and TBMCS systems administrators. With WMs close at hand, these system administrators were able to focus on higher-level network support requirements. Operational users experienced greater productivity with reduced system downtime than in JEFX '98 and '99. Operational availability of the network and information on the network proved crucial to the success of time-sensitive targeting and decision-making.

Once the operators arrived at the three primary

CAOC locations, Hurlburt Field, Fla.; Nellis AFB, Nev.; and Langley, the WMs concentrated on two key tasks. First, they determined what, when and where information was needed by decision-makers, and second, how to manage information to meet decision-makers' needs. This was a tremendous challenge, as several applications were providing the same functionality, and users tended to migrate toward the one they were most comfortable with. Additionally, the lack of business rules and standard roles-based user profiles, interoperability problems between NT and Unix systems and applications, and "just-in-time" training for users and WMs alike, created the ingredients for disaster.

The WMs determined how information could best be distributed and displayed through user-defined information requirements and the numerous information tools available, such as TBMCS, LiveLink, Web pages, collaborative tools, e-mail, and other tools. With very limited space and telephones to work with, the first task was to set up standards and a process for getting WM assistance and accessing, distributing, and storing relevant information. Next they gathered information requirements from the operators and senior leaders to facilitate decision-making.

Commander policies governing use of information access and communications systems was critical to ensuring information availability when the decision-makers needed it. Restricting Internet usage, message distribution policy, application access and permissions, file storage policy, and other measures optimized bandwidth use and information exchange. These control mechanisms provide commanders the ability to use information management as a force multiplier.

WMs worked with their WM Webmasters, TBMCS and Info Workspace system administrators at the Help Desk and in the NCC to establish and modify user accounts, and build file plans, directories, and Web pages to make information transferable and processes manageable across both UNIX and NT operating systems. Collectively, they built 16 Web-enabled tools to manage problem reporting, battle rhythm (scheduling), air tasking orders production, significant events, requests for information, Ops Intel logs, suspenses, personnel locator, recall rosters, telephone books, records, Web pages, e-mail groups, INFOCONs, anti-viruses, and AFCERT kick scripts. These tools and systems allowed operators to present their information with minimal effort in real time.

## Rain, sleet, wind don't deter communications support



*Photo by Tech. Sgt. Orville Desjarlais*

**Members of the host base team at Tinker AFB, Okla., walk across frozen ground during a local exercise.**

**By Tech. Sgt. Orville Desjarlais**  
*552nd Air Control Wing Public Affairs*  
*Tinker AFB, Okla.*

Their support role is rarely in the spotlight. In fact, providing a host base environment is not part of their communications mission.

But the men and women of the 552nd Computer Systems Group “stepped out” and endured the 12-and-a-half-hour shifts, the below-freezing temperatures, the gas mask exercises and working in tents to provide a realistic training environment to ensure that the E-3 AWACS team is ready to deploy worldwide.

With rain, sleet, snow and freezing weather and wind, providing 24-hour support for AWACS fliers and maintainers was more challenging than usual during a recent Sentry Leap exercise. The exercise focused on readiness, reliability and sustainability while deployed to a forward-operating location that had both chemical and terrorist threats.

It's the host base's job to provide Contamination Control Area processing, casualty collection and personnel accountability, arrange for meals ready-to-eat

and hot food, and to have tents erected so that exercise participants have a place to escape the wind and snow while training and exercising their ability to survive and operate in a combat environment.

“I was really proud of our people who had to work in the ice and snow,” said Lt. Col. Nancy Bettis, 552nd Computer Systems Squadron commander, who served as the host base support commander. “We accomplished our host base support responsibilities to provide the needed combat functions that the 552nd Air Control Wing doesn't deploy with.

Host base support is a combined effort among the 552nd Computer Systems Squadron, the 552nd Computer Systems Group, the 752nd Computer Systems Squadron, along with members from public affairs, medical, life support and logistics functions. During an operational readiness inspection, inspectors only grade the life support function, but the missions of the rest of the host base functions are no less important.

During a Sentry Leap exercise, the host base is simulated to be located about 15 kilometers from Base X, where the AWACS crews and maintainers are deployed. All air missions are flown from Base X. But

when operations or maintenance crews need a break from the elements, they travel to the host base to get out of the snow and wind and get a warm meal. They must also visit the host base to enter and exit the exercise area, have simulated and real world medical problems tended to, and to perform personal decontamination procedures.

Accomplishing host base support requires a lot of time and people. It takes about four weeks to support each exercise: two weeks of planning, preparing and setting up; one week of execution; and the last week tearing down and packing up. About 150 people are needed to build, run and dismantle the host base.

“The CSG troops are very proud of the wing’s partnership and are glad to step out and help provide our wing realistic training,” said Colonel Bettis. However, leaving an office means leaving work behind. “We recognize that some work may be delayed, such as developing software enhancements for AWACS, but taking part in exercises is important. It’s not easy staying in tents and ‘sucking rubber’ during gas mask exercises, but these exercises improve our situational awareness and create realism for our troops who deploy into harm’s way. We must ensure that our wing is always ready to deploy and survive in any hostile environment. The

members of host base support create a viable toxic-free environment during the exercise to maximize training benefits,” said Colonel Bettis.

Supporting these exercises makes it tougher for people left behind in their normal work centers, because they have to take up the slack for those in the exercise.

Is it all worth it?

“We get a lot of positive feedback from the players as well as wing leadership,” said Colonel Bettis. “Everyone appreciates the support facilities we provide, especially the hot chocolate and hot meals.” The Inspector General also recognizes the valuable contributions of host base personnel. “Despite most of our functions being non-graded, as well as not our peacetime mission, the IG recognized our teams for nine Superior Performance Team awards during our April 2000 Operational Readiness Inspection,” Colonel Bettis added.

She said it’s the enthusiastic people on the host base support team who are responsible for all our successes. “They’ve done this so many times that they’ve got it down pat.” There are about four Sentry Leap exercises scheduled throughout the year. And exercising alongside everybody else – in the tents and foul weather — will be the host base support team.



*Photo by 1st Lt. Christine Frey*

**E-3 exercise maintainers change a tire minutes before a simulated chemical warfare attack at Base X during the exercise.**

# Recon imagery

## No need to fear unit's arrival

By Staff Sgt. James A. Rush  
332nd Air Expeditionary Group  
Public Affairs  
Ahmed Al-Jaber Air Base,  
Southwest Asia

The kids on the softball field here lost a ball the other day. A batter pulled a foul ball deep down the left field line and it landed inside a compound that had mysteriously appeared almost overnight.

The ominous razor wire fence kept anyone from getting up the nerve to knock on the front door to ask for the ball, but the fear wasn't necessary. The new neighbors, while secretive, are quite friendly.

The 9th Intelligence Squadron (Deployed) from Beale AFB, Calif., moved in recently much to the benefit of the fighter community here. The intel trailers house photo-processing equipment to develop pictures taken by reconnaissance aircraft, according to Capt. Scott Strohecker, the deployed unit's commander.

Moving the 9th Intelligence Squadron folks to the region speeds the process significantly, said Master Sgt. Cindy Spinks, assistant superintendent of imagery exploitation. "It shortens the time lines; otherwise the film would have to go back to the states," she said.

After film is processed, sharp-eyed intel people "exploit" the images and report their findings back to higher headquarters. The faster turnaround makes it easier for commanders to assign missions to units in the region, Sergeant Spinks said.

On the unit's first "real-world" deployment since Desert Storm, being so close to the action is a big moti-



Photo by Staff Sgt. James A. Rush

**Staff Sgt. Brian Smith checks film to make sure it wasn't scratched during processing.**

vator for the deployed team.

"We know people are looking at our products and we get feedback," Captain Strohecker said. "We know they like what we're doing. That's a pretty good feeling."

The portable photo lab is here at the request of U.S. Central Command. More than 30,000 feet of film has been developed since it arrived. The around-the-clock operation has been busy. Despite that, the intel specialists are keeping a good attitude.

"We're pretty excited to be doing a real-world mission," the captain said. "It's a big morale boost for the troops."

Maybe it's OK to go get that ball after all.

# DOD gets global with satellite-phone system

By Gerry J. Gilmore  
*American Forces Press Service  
Washington*

The Department of Defense awarded a two-year, \$72 million contract Dec. 6 to a Maryland firm for unlimited use of its global, satellite-based, secure telephone network.

The contract was awarded through the Defense Information Systems Agency to Iridium Satellite LLC (IS) of Arnold, Md., which will contract with the Boeing Co. to operate and maintain the system's 73 satellites.

According to Dave Oliver, Principal Deputy Undersecretary of Defense for Acquisition, Technology and Logistics, the contract will give DOD increased communications ability around the globe and a conduit to private-sector innovation.

Under the contract, DOD will pay a \$3 million monthly service fee for unlimited airtime for 20,000 government users over the Iridium satellite network. Contract options, if exercised, could increase the contract value to \$252 million and extend the contract period to 2007.

"Iridium will not only add to our existing capability, it will provide a commercial alternative to our purely military systems," he said. "This may enable real civil-military dual use, keep us closer to the leading edge of technology, and provide a real alternative for the future."

The system offers state-of-the-art satellite communications service to any open area in the world. It provides mobile, cryptographically secure telephone services to small handsets anywhere in the world, North Pole to South Pole, 24 hours a day, officials said. They noted the system and its DOD-specified enhancements will provide handheld phone service not currently available.

Officials said the system can improve the capabilities of special forces operations, combat search and rescue activities, and polar communications. It also can enhance DOD's mobile satellite communications requirements.

Motorola designed, built and operated the \$5.5 billion Iridium system. The system went into operation in November 1998, and DOD used some 800 of its first-generation phones. The Motorola-owned unit, Iridium LLC, was charging some of its 60,000 customers up to \$5 a minute for calls when it went bankrupt in August 1999. Iridium Satellite LLC recently bought the bankrupt company's assets.

Mr. Oliver remarked that subsequent advances in technology, an expanded customer base, and savings in start-up costs enable the new owner to provide commercial service for about 80 cents a minute, while the Pentagon will pay 10 to 30 cents a minute. He said company officials estimate they will "break even" with 40,000 more customers and expect to service 250,000 within five years.

The original Iridium handset is boxy and bulky, Mr. Oliver said.

An improved model by Motorola, he continued, is about twice the size of a typical cell phone and has a call-reliability rate of 95 percent. Its special encryption sleeve ensures secure communications, he added.

Motorola will continue to supply DOD with handsets and parts for the time being.

The U.S. military will use its Enhanced Mobile Satellite Services Gateway system at Wahiawa, Hawaii, to provide DOD Iridium users with direct-dial connection to the Defense Information Services Network and to public-switched telephone networks, officials said.

## Where do we go from here?

By John Holliday  
*3A031 IM Apprentice Instructor,  
Keesler AFB, Miss.  
and Master Sgt. Raymond  
E. Moore  
Installation 3A0X1  
Functional Manager  
Hill AFB, Utah*

To understand who **WE** are, let's go back several years. Information Management is a time-honored career field that can proudly boast of being the only specialty in the Air Force that provides services and support in every functional area, at every echelon. Not only do we conduct effective and efficient Information Management programs in hundreds of flights, squadrons, groups, wings, etc., but we also provide integral management and support within command headquarters, the offices of the Chief of Staff, Secretary of the Air Force, Secretary of Defense, and our Commander-in-Chief, the President of the United States.

Historically, the Information Management career field has always included a broad area of job functions with a wide variety of responsibilities. Since its beginning in 1952, there have been a number of major and minor classification changes. From 1952 to 1956, members of the 702X0 career field were called Clerks. This title was changed to Administrative Clerk in 1956, then Administrative Specialist in 1970.

Another major classification change took place in 1977.

See IM Page 25

# *SWA's special instructions to communicators help operationalize, professionalize deployed communications business*

How do you provide the warfighter sustained communications support while rotating 1,800 communications personnel through the theater each year?

The Joint Task Force-Southwest Asia Communications Directorate, under the leadership of Col. Mike Basla, developed a two-phased approach to address this problem and stabilize the communications operating environment within the Southwest Asia area of responsibility.

First, the directorate developed and published the Special Instructions to Communicators. This document uses fundamental operational

concepts to maintain stability and continuity of operations throughout the AOR. These operational concepts or Communications Centers of Gravity are the foundation for all communications operations within the AOR. The 74-page document builds upon the Communications Centers of Gravity to provide field units guidance on a variety of topics, including outage reporting, frequency allocation, INFOCON actions, network virus response and configuration management.

Another important facet of the SINC is the daily Communications Tasking Order which helps direct

day-to-day operations and maintenance throughout the AOR. The CTO authorizes maintenance outages, provides deployed units daily taskings, and establishes the current INFOCON posture. When combined the SINC and the CTO provide communicators both strategic and tactical guidance for operations within the AOR.

To ensure field commanders have the tools to execute their SINC and CTO missions, the Directorate developed the Joint Job Qualifica-

See **SPECIAL** next page

## Reservists tapped to fill new info ops units

By **Gerry J. Gilmore**  
*American Forces Press Service*

WASHINGTON – DOD plans to recruit hundreds of Reserve Component information technology specialists in coming years to fill positions in several new military “cyber-security” organizations, under plans approved by the deputy defense secretary.

Deputy Defense Secretary Rudy de Leon recently provided the go-ahead to establish five joint Reserve virtual information operations and Information Assurance organizations to ensure that American warfighters dominate the military computer information realm in future conflicts.

“Information operations has emerged as an area that is extremely well-suited to integration of Reserve capabilities,” Mr. de Leon said in a press release. “Members of the Reserve and National Guard are often way ahead by the very nature of their civilian employment, trained in their workplaces to exploit technology.”

DOD needs 182 Reserve Component officers and enlisted members to man the five organizations for fiscal 2001 and 2002, officials said. Numbers of people in each organization will vary. The total number of people in the units is expected to grow to more than 600 through fiscal 2007.

The Reserve Component technicians and their units will support the Defense Information Systems Agency, and the Joint Task Force-Computer Network Defense,

Arlington, Va.; the National Security Agency, Fort Meade, Md.; the Joint Information Operations Center, Kelly AFB, Texas; and the Information Operations Technical Center, Fort Meade, Md.

The need for DOD to safeguard its computerized information systems is illustrated by recent “cyber warfare” between Israeli and Palestinian computer technicians featuring the defacing of opponents’ Web sites and massive jamming of digital information conduits by e-mail saturation and virus mail.

The decision to upgrade DOD’s information security infrastructure originated from a recommendation from the Reserve Component Employment 2005 study, which suggested new ways to employ Reserve forces as part of fostering improved integration in the Total Force, said Charles L. Cragin, Principal Deputy Assistant Secretary of Defense for Reserve affairs.

He noted that Reserve Component members who work for info-tech industry firms like Microsoft and IBM will be good fits for the new organizations.

“The virtual information organizations are another recognition of the expertise of members of our Reserve community that may not necessarily be an area where we can retain a lot of people on active duty,” Mr. Cragin said. “We have a number of people in the Reserve components that have that sort of technology.

“They have a very patriotic desire to continue to serve their country. We want to be able to utilize their expertise,” he concluded.

## IM

*From Page 23*

The administrative career field was divided into three shred-outs. The three shred-outs were given the following titles:

**702X0A** - Administration  
Management

**702X0B** - Staff Support  
Administration

**702X0C** - Orderly Room  
Administration

Duties involved telephone etiquette, taking messages, greeting visitors, scheduling appointments, Airman Performance Reports, Officer Effectiveness Reports, maintaining unit locator files, issuing and controlling meal cards, processing requests for BAS, maintaining unit leave records, monitoring the INTRO program, and personnel actions, just to name a few.

In 1984, the three shred-outs were again united into one career field, keeping the title of Administration Specialist. In 1989, this title was changed to Information Management Specialist to more accurately define the actual work.

Then, on Oct. 31, 1993, the Air Force implemented a revised classification structure for everyone, and our career field or Air Force Specialty Code was changed from 702X0 to 3A0X1.

There was a time in my 19 years of service, I can remember being called the "702", "Radar O'Reilly", "admin troop", "tech admin", "admin specialist", "admin tech", and "secretary." I remember the days when I was asked, "What exactly is your

job?" "Someone would reply, "His job is to answer the phones and greet visitors." This is the year 2000, and I still hear new Information Managers contacting me that someone in their organization has told them that answering phones and greeting visitors is their primary duty.

I am an Information Manager! In fact I'm proud to be an Information Manager who has spent over 19 years in this career field. It has been tough at times, however, I chose to stick it out until that one day when I would be in a better position to assist my fellow Information Managers. As an Information Manager, I have been where they are now. I have sat in those same seats and said, "No I'm sorry, no one is in at the moment, can I take a message?" "I can't go to lunch right now because I have to answer the phones until someone returns." I believe our biggest concern in this career field is that we are misunderstood. We fail in this area because we do not take the time to educate our commanders, supervisors, and peers on the uniqueness of our career field. There are even those times when we are not sure which path we are taking. Whatever the path, we continue to provide exceptional support to the Air Force mission.

The year 2000 is upon us and the career field is still taking drastic turns (for the better). Our Information Managers can look forward to workgroup management that will definitely compliment our existing career field. Our new path will take us down a road that will open new doors using electronic forms, elec-

tronic records keeping, web page development, operationalizing and professionalizing the network, computer familiarization and configuration, information assurance, essentials of networking, computer protection, software installation, and databases. This new training will continue to enhance our current knowledge, bringing workgroup management into the forefront of our career field, replacing the "old" ways of doing business. Our Information Managers are more than willing and capable in taking on this additional training. We must allow our Information Managers the opportunity to grow and develop as Information Technology continues to grow and develop. In the long run, this new training will only give our commanders a more rounded and professional force equipped and trained to meet the ever-growing world of Information Technology.

At Hill AFB, our Information Managers are taking the lead in the future of our growing technology. Currently, we have Information Managers in 649th CLSS and 649th MUNS managing the Network/LAN shop; an Information Manager in 75th MSS as the workgroup manager; an Information Manager as the assistant chief of the Help Desk, Information Managers as instructors for base workgroup management and the Operationalizing and Professionalizing the Network Regional Training Center. If given the opportunity and training, all Information Managers can continue to provide their units with valuable benefits to the success of the Air Force mission.

---

## SPECIAL

*From previous page*

tion List. The JJQL will ensure the communicators filling positions in the AOR possess the necessary skill sets to overwhelmingly support the warfighter. In future deployments, communicators must meet JJQL standards before deploying into the theater.

These two documents are the cornerstones for the Directorate to improve communications operations within the theater. Therefore, all communicators are

required to familiarize themselves with these documents before deploying to the AOR. Additionally, ingarrison commanders must certify their personnel understand the SINC before deploying to the Southwest Asia AOR.

These documents are available on the Web at [wwwmil.jtfswa.af.mil/j6/j63.htm](http://wwwmil.jtfswa.af.mil/j6/j63.htm). For additional information or questions, please contact the JTF-SWA/J6 Standardization and Evaluation officer, DSN 318 435-7865.

# Non-stop action helps comm group improve deployments

By Tech. Sgt. Andrew Gates

*5th Combat Communications Group Public Affairs  
Robins AFB, Ga.*

As the Air Force rolls into the second Aerospace Expeditionary Force cycle, members of the 5th Combat Communications Group can be proud of their efforts to improve the rotation process.

The group has been involved in every rotation since Cycle 1 began in October 1999, according to Master Sgt. Timothy Birdsell, group deployment manager.

The Expeditionary Aerospace Force concept isn't as new to the 5th CCG as it is to other Air Force units, said Capt. Roosevelt Boyland, chief of the plans and operations flight of the 5th Combat Communications Support Squadron. "EAF is based somewhat on our unit

integrity program — a concept the 5th has used for several years."

What the AEF process did provide for the group was even more stability, according to the captain. Under the unit integrity program, the group's squadrons could, and did, draw from one of the other three mission squadrons to help meet their requirements. Under the rules for AEF, that is eliminated. "If a squadron can't meet a requirement, we now send it back to the AEF Center," said Captain Boyland.

"We will augment, as necessary, from the group's support squadron," Sergeant Birdsell said. "There are still a few career fields that are critically short, and we just don't have enough people in each of those fields in

See **ACTION** next page



*Photo by Tech. Sgt. Andrew Gates*

**Airman 1st Class Michael Stamper, left, and Airman 1st Class Jake Pelletier, both from the 52nd Combat Communications Squadron, set up the Hammer Rapid Initial Communications Kit satellite antenna during a recent 5th**

**Combat Communications Group exercise. The Hammer RICK is used to provide quick-reaction command, control and communications information during emergencies or contingencies.**

## ACTION

*From previous page*

our mission squadrons.”

The continual process of deployment and return has been beneficial for the group. Since it is regularly involved in the process, members of the group have a relatively unique role in improving AEF cycles, according to Captain Boyland. “Since we are continuously involved in sending people on deployment, we can help fix issues that a unit that only deploys once every 15 months doesn’t necessarily see.”

The most visible evidence of this is through feedback questionnaires after each rotation, Sergeant Birdsell said. “We regularly attend conferences and meetings to make sure the entire process works as smoothly as possible.”

Since Cycle 1 began more than 15 months ago, the people of the 5th have seen an increasingly smoother process, the deployment manager said. That doesn’t mean everything is perfect just yet.

When problems do emerge, however, communication between the 5th CCG, the Aerospace Expeditionary Force Center, and the requesting unit is crucial to mission success, according to Captain Boyland. The communications process allows for quick and fair ways to address emerging concerns.

“For instance, the 5th has some incredibly talented and well-qualified 3-level airfield people. In previous rotations, we were deploying mainly to (Southwest Asia) — and the people there were focusing on the experience and abilities our people had, not their training level. When we started moving our people to areas managed by U.S. Air Forces in Europe, USAFE requirements focused on the skill-level rather than the

deployee’s actual abilities. By continuously communicating through the Aerospace Expeditionary Force Center, we were able to address this situation before it became mission critical. We also gave other deploying units some information on another command’s requirements.”

Other suggestions and improvements may not be immediately solved, but can improve the process in the long run. Sergeant Birdsell relates an improvement which should be implemented by Cycle 3, starting in March 2002. He describes a recent meeting at Langley AFB, Va., where the goal was to develop smaller Unit Type Codes (deployment requirements) for base communications units.

“Right now, Air Force communicators fill about 4,000 slots per year for contingencies,” he said. “These slots tend to be large groups, entire communications packages. The meeting attempted to shrink those requirements to three or four people -- which should make it easier for other communications units to fill those UTCs

while accomplishing their daily home-base mission. If they need four people for a network control center, they can draw those four people from one unit by using one UTC.” This refines the focus of each UTC and should make it easier for units to support taskings.

“The bottom line is that our mission is to deploy, set up and sustain tactical communications,” said Lt. Col. Don Mertz, 5th CCG deputy commander. “That’s our job. It behooves us to make sure the deployment process is as smooth and predictable as possible, for both ourselves and others.”

Life slows down some for the group in March, when all four mission squadrons are expected to be home for three months. That hasn’t happened since the beginning of Operation Desert Storm in 1991.

**“Since we are continuously involved in sending people on deployment, we can help fix issues that a unit that only deploys once every 15 months doesn’t necessarily see.”**

*Capt. Roosevelt Boyland,  
5th CCSS*

---

## C&A

*From Page 7*

ing a JTA-AF migration plan within 90 days). If the conditions are not satisfied, the base DAA may opt to disconnect the system.

The certification process doesn’t stop there. Once a Certificate of Networkiness is issued, the system then goes to the MAJCOMs for a Certificate to Operate. For MAJCOM CIOs to issue a Certificate to Operate, they look at MAJCOM unique issues such as their base’s infrastructure, host nation support agreements, funding and training, to name just a few. And if everything is in place, the CIO

may issue a Certificate to Operate.

Without an approved Certificate of Networkiness signed by the Air Force CIO, and a Certificate to Operate signed by the MAJCOM CIO, a system will not be connected to the Air Force Enterprise Network. There should be no more instances where systems “just appear” without notice, without planning, and expecting everything to be in place.

The Air Force C4ISP, Certificate of Networkiness, Certificate to Operate process is still in its infancy and a few MAJCOMs have not implemented a Certificate to Operate process. A few bases are already feeling the effect of the Certificate of Networkiness and Certificate to

Operate process with new functional systems coming on line. No longer must each base complete a C&A; rather each new system will have a signed Certificate of Networkiness and a Certificate to Operate. Thus, with the entire Certificate of Networkiness and Certificate to Operate package appearing with the functional system, the base DAA can make an informed decision on a functional system before it’s connected to the network and made operational. All that must be done locally is site certification, including unique issues associated with each base, which is a lot easier and less time consuming than an entire C&A.

**"Emphasizing the importance  
of IA in all we do, the Air Force  
is embarking on a year-long  
Information Assurance  
Awareness Campaign ..."**

Lt. Gen. John L. Woodward Jr.  
Air Force Deputy Chief of Staff  
for Communications and Information