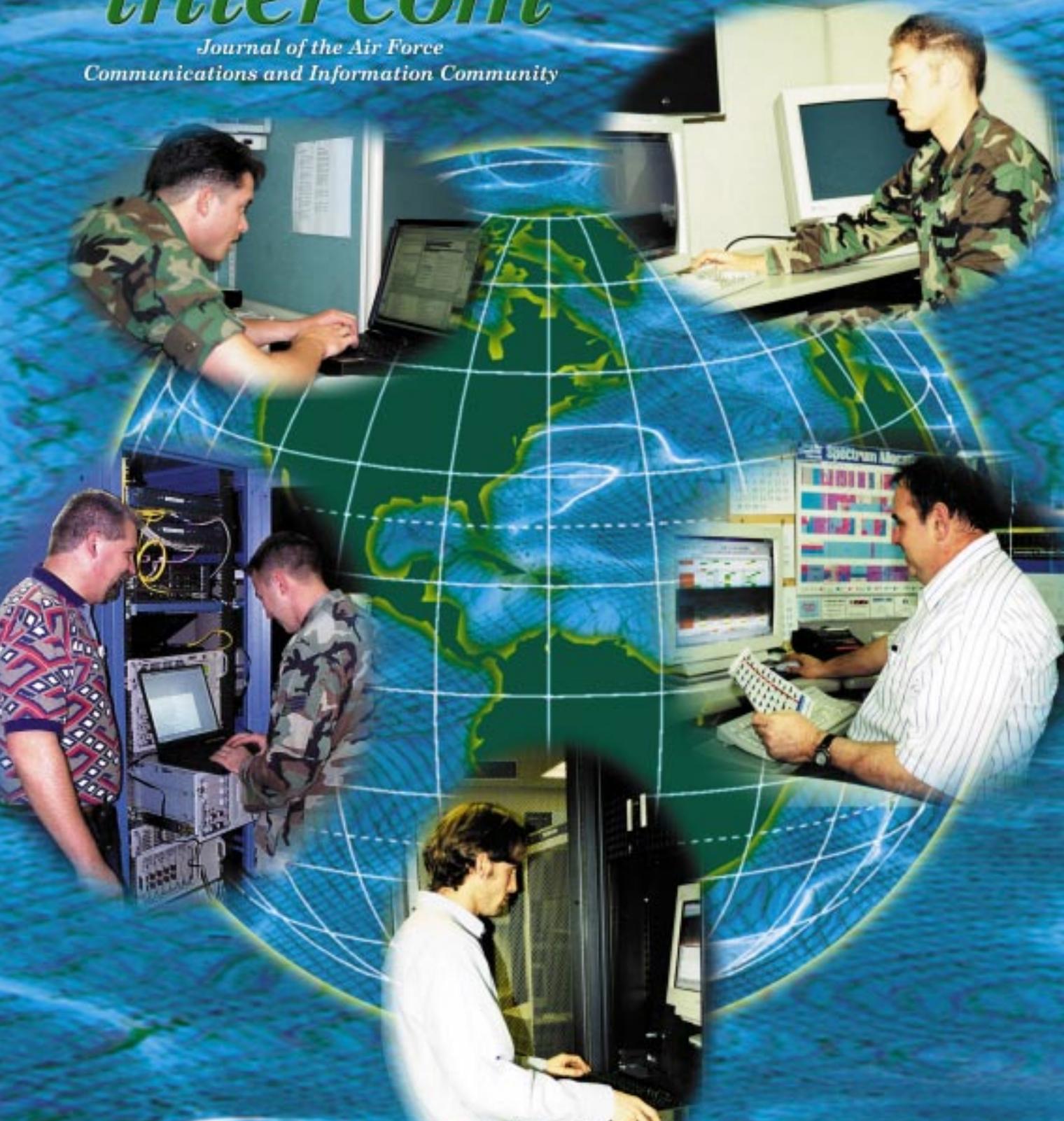


March 2001

intercom

*Journal of the Air Force
Communications and Information Community*



*Scope Net
fine-tuning base networks*

intercom

Volume 42, No. 3

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, 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/>



Scope Network

3 Scope Net teams reinforce effective base network operations

IA Awareness Campaign 2001



8 'Digital Devices' is March theme for IA Awareness Campaign 2001

10 Viruses affect personal digital assistants and networks

11 Protecting and accounting for personal digital assistants

12 Digital copiers: intelligent peripherals that pose a significant threat

14 IA awareness, training and education: Do you know the differences?

15 Carl von Clausewitz on information in war: a matter of trust



IT focus group

16 AF Enterprise Directory Services: powering the network

in other news

18 Senior communicators formulate direction of AF IT Enterprise

19 Dynamic Network Analysis toolkit automates network planning and analysis functions



20 Air Force enters new era with portal

22 Program puts war info at fingertips

24 Confining contacts with contractors

27 Pentagon comm member's work earns him a promotion

30 Former AFCC member dies

features

31 Sergeant gives brother gift of life



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

About the cover

Scope
Net teams
help fine-
tune Air
Force base
networks.



Cover by Tech. Sgt. Mike Leonard

Scope Net teams reinforce effective base network operations

By Len Barry

*Air Force Communications Agency Public Affairs
Scott AFB, Ill.*

Scope Network is a small group of dedicated people with a big job: helping to keep one of the Air Force's most important weapon systems – the network – up



Photo by Tech. Sgt. Mike Leonard

Tad Barncord, Scope Net Support Branch contractor, performs server administrative functions on the Scope Net Support Branch server.

and running at peak performance at bases worldwide.

Ten teams of four individuals from the Air Force Communications Agency's Global Connectivity Directorate, at Scott AFB, have the monumental task of traveling to 110-120 bases for one week each year to:

- Tune the network for optimum performance.
- Enhance network security.
- Improve operations management.
- Train and mentor technical personnel.
- Identify and share best practices.
- As required, respond to emergency situations.

In every instance, they leave the base network in better shape than they found it.

Needless to say, the word that "Scope Net (for short) is on the way" is music to the ears of commanders, network administrators, technicians and last, but not least, computer users.

"In my opinion, Scope Network is a super tool that's paying off big for the (Air Force information) enterprise," said Maj. David A. Rearick, commander of the 509th Communications Squadron, Whiteman AFB, Mo., after a recent visit. "This was my first experience with Scope Net and the people were extremely knowledgeable and team-oriented. They confirmed or iden-

See **SCOPE NET** Page 4



Photo by Thomas Partelow

Scope Net's 1st Lt. Dan Korstad (foreground) trains team member 2nd Lt. Ben Richeson on firewall troubleshooting and configuration techniques, while Senior Airman Shane Canell, Davis-Monthan AFB, Ariz., network control center, looks on.



Photos by Tech. Sgt. Mike Leonard

1st Lt. Mike Reavey, Scope Net team member, checks his notes for past Profiler software configurations, while working in one of Scott's communications hubs.

SCOPE NET

From Page 3

tified numerous configuration adjustments, helped us repair or identify new managerial tools, and provided suggestions to enhance our information protection posture," he explained. "Their sole objective was to help us



Thomas Partelow, Scope Net team chief, checks the travel schedule.

optimize Whiteman network operations and I was pleased with the results," Major Rearick said.

Another unit, visited last month, had similar comments. "I've worked with Scope Net twice – both here and in South-west Asia, and they helped us out a lot both times," said Lt. Col. Curtis V. Frost, commander of the 5th Communications Squadron, Minot AFB, N.D. "They're an important factor in our operations. It gives you a good feeling to have the experts come out and confirm how well you're doing." Colonel Frost added, "They evaluated our net, helped solve a congestion problem and made a few minor tweaks. They're a good, solid team, and I'm very pleased with the support and services they've provided for us."

Scope Net began as strictly a rapid response operation in

July 1997. Then in August 1998, it geared up a program of scheduled base visits, beginning with eight teams in January 1999. The teams started out spending two weeks at each base every two years. Then last month the number of teams grew to 10 and the new schedule includes a one-week visit to each base once a year. The teams move constantly throughout most of

the 48 states, Alaska and Hawaii, to as far afield as Saudi Arabia, Turkey, Italy, Spain, Germany and the United Kingdom, as well as the Azores, Greenland, Japan, Okinawa, Guam and Korea. Each team currently averages 12 trips annually. They are organized by major command, so that each MAJCOM has a designated Scope Net point of contact. Each visit must be scheduled not only with the base concerned, but also with the respective MAJCOM headquarters.

The six members of the Scope Net Support Branch at Scott coordinate schedules, and assure each team has the hardware, software, licenses and tools it needs to get the job done. Some countries have more restrictions than others, making the coordination task more difficult.

The four team members typically include:

- * A communications officer, nor-

1st Lt. Travis Howell and Tech. Sgt. John Caterino, Scope Net team members, test an optimized network management configuration on a simulated base network using HP Openview.



Photo by Tech. Sgt. Mike Leonard

mally a captain or contractor, specializing in operating systems, applications and e-mail.

* A communications engineer, normally a captain or contractor, specializing in routers, asynchronous

transfer mode, switching and protocols.

* A network technician, normally a technical sergeant or contractor, specializing in information assurance.

* A network technician, normally a technical sergeant or contractor, specializing in network management.

The team is sometimes augmented by a fifth member, usually a newly-assigned lieutenant who specializes in training and serves as a team understudy.

The teams have a set of standard objectives and procedures, but also tailor the focus of their visits to the particular requirements of the unit visited. Each base submits a needs list 30 days prior to the team's arrival.

In addition to the regular base visit program, Scope Net provides advice and assistance by phone, remote access, and on some occasions, by making a rapid response visit to units with emergency situations. Composition of rapid response teams depends on the needs of the situation and the expertise of the available team members and may include members of the Base Assistance Team at Maxwell AFB-Gunter Annex, Ala.

Scott Gardner, a current team member who's been with the program from the start, helped define Scope Net's mission in layman's terms. "Officially, we enhance communica-



Photo by Thomas Partelow

Steve Eales, Scope Net contractor, coordinates router and switch configuration changes and provides training to Senior Airman Lawrence Nicholson, 355th CS, at the Davis-Monthan network control center.

See **SCOPE NET** Page 6

Stan Grant, Scope Net contractor, discusses optimizations for Scott's local area network with Tech. Sgt. Lisa Davis (center) and Staff Sgt. Patricia Ford, 375th CSS.



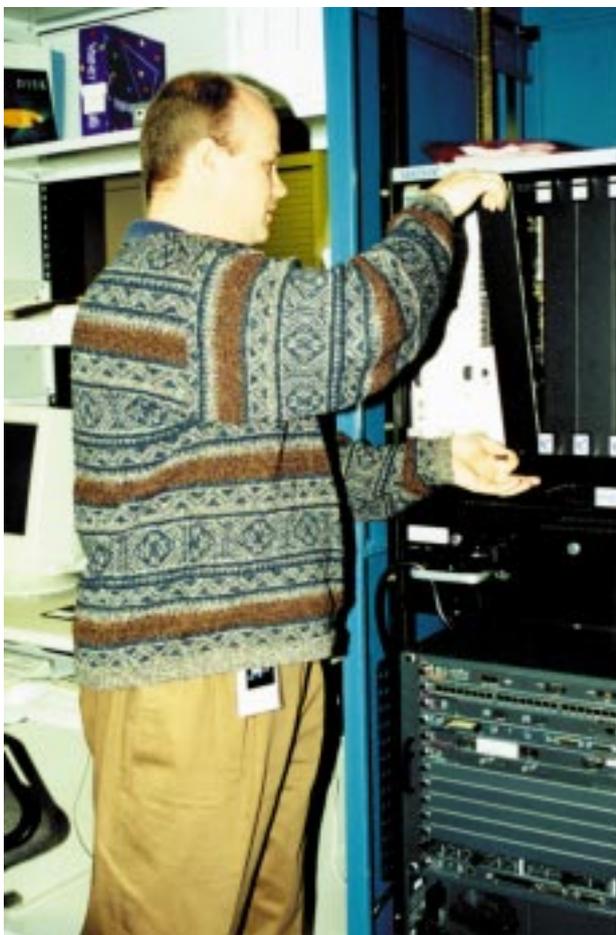
Photos by Tech. Sgt. Mike Leonard

SCOPE NET

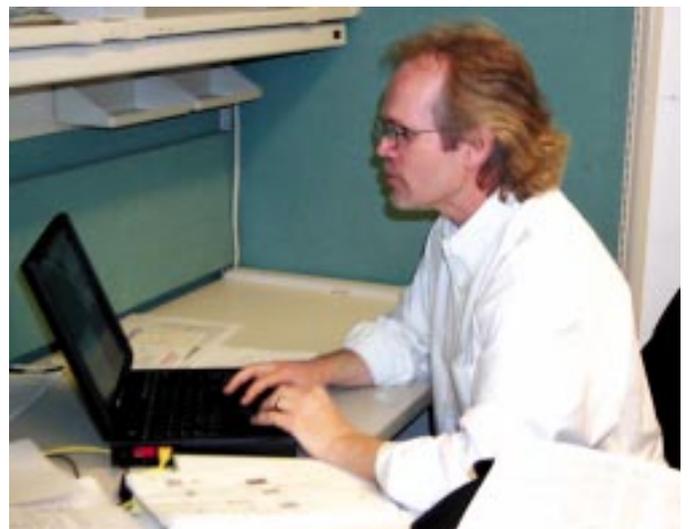
From Page 5

tions operations by optimizing the base's local area network. In other words, we 'tune up' the LAN."

Typically, the teams discover software or equipment that's badly installed, improperly configured, incompatible with other system elements, or simply outdated. Broken or damaged wires can also cause disruptions. "In some places, we've gone into a comm closet – it's usually a dark place, and may be in an older building that's not necessarily well sealed – and found cables have been gnawed by an animal such as a rat or gopher," Gardner said. The network can also be bogged



Jay Dentmon, Scope Net contractor, checks a blade on a router in the AFCA Scope Network lab.



AFCA contractor and Scope Net team member, Chet Ratcliffe, checks the Scott AFB network firewalls.

down with unnecessary software programs that are standard features of the system. "These extra protocols take up bandwidth (data communications space) and don't buy you anything," he added.

"In the worst cases, we've found networks operating at one-tenth of their capacity because of these kinds of problems," Gardner said.

Gardner recalled two occasions that required a rapid response team to deploy. "In one case, senior management couldn't get to their e-mail from home. The router (remote access server) was not configured right, so we replaced the core software, recommended a long-term solution and fixed some other problems while we were there," Gardner said.

"Another time there was a network that was really sluggish," Gardner said. "They had a bunch of old equipment that was connected the wrong way. We provided a temporary solution and gave them a list of equipment they needed for a permanent fix.

"We get calls all the time about things that don't require us to go out. For example, one base said they were having trouble with their telephone switch not talking to their remote server. It turned out they had replaced their old server with a new one that used a different protocol. We did some research and figured it out, and fixed the problem over the phone," said Gardner.

As with any line of work, being a member of a Scope Net team has its pluses and minuses.

"The toughest part of the job is the rapid turnaround required," said Tom Partelow, a Scope Net team chief. "When we get back from a (one-week) trip, we typically have one week to finish our report, one week off, a week to prep for our next trip, and then we're back on the road."

"The biggest challenge is that we travel a lot – about 100 days a year. It's a very fast-paced organization," Gardner said. "On the other hand, it feels really good to go out and actually help people. You can fix something and see the results. The base is usually happy to see you come and glad you came. Another nice thing is that you get to see a lot of places you'd never see otherwise. Those are the rewards."

Looking ahead, there are no foreseeable changes on the horizon for Scope Net. "Now that we've visited every base, we've laid some groundwork and established a reputation, so that will make future visits smoother," Gardner affirmed. "We should no longer have to answer questions like, 'Who are you and why are you here?'"



Photo by Tech. Sgt. Mike Leonard

Tanya Ott, Scope Net Support Branch contractor, formats a spreadsheet containing a profile of base network traffic.



Photo by Thomas Partelow

Capt. James Darby, Scope Net team chief (left), and Senior Airman Lawrence Nicholson, 355th CS, Davis-Monthan AFB network control center, troubleshoot a connectivity problem during prearranged network downtime at the base.

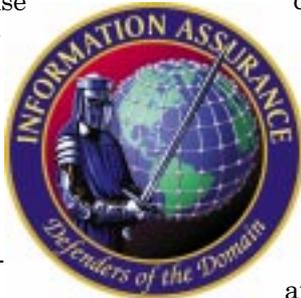
'Digital Devices' is March theme for IA Awareness Campaign 2001

By Col. William T. Lord

*Director of Communications and Information
Air Mobility Command, Scott AFB, Ill.*

The security of Air Force networks depends on you. Without it, we can't leverage the immense power of information to increase the lethality of our warfighters. Throughout the year, the entire Air Force is focusing on a unified campaign, Global Vigilance, Reach and Power: Information Assurance in the 21st Century. This campaign is important to our Air Force because the next "Pearl Harbor" is likely to begin with a massive assault on our information systems.

Because of our increased reliance on computer networks to defend our nation, each military member, civilian employee and contractor must constantly remember when one person uses poor security practices,



they impose increased risks on all who use our networks. With this in mind, please don't become the weak link in the security of our networks. Make a continual effort to identify and eliminate any weak security practices. And help your co-workers by taking time to correct them when they use improper practices. By making a continuous, conscious effort to improve security, you're doing much more than protecting your official e-mail or your administrative word processing files. You are protecting entire networks which have become integral to our national defense.

I encourage everyone to participate in and contribute to the 2001 Information Assurance Awareness Campaign activities, as the Air Force continues to provide world-class information superiority to warfighters. With diligence, we can stop the next Pearl Harbor before it begins.

Know the risks of personal digital assistants

By Senior Master Sgt.

Alan McClellan

*Air Mobility Command
Scott AFB, Ill.*

"Oh, man! What happened? Last year we had Information Assurance Awareness Month in February, and this year we have a continuous campaign of security-related articles and events every month! I already have a job that keeps me very busy without any of these scheduled distractions, so why do I need this information?" Have you heard or even made some similar comments?

As an Air Force member, civilian employee, or contractor who accesses any form of government information system, you must keep current on security requirements. Your lack of knowledge about new security requirements within the arena of national defense could prove costly. Within the Air Force,

ignorance of new regulations and requirements is not necessarily an airtight defense, if you have played a role in compromising sensitive information or impacting entire networks.

Rapid technological changes have heightened the need for observation of information security practices in regard to personal digital assistants. Air Mobility Command will face several issues regarding PDAs during 2001. With the reduction of personnel and defense funding during the past 20 years, national defense increasingly depends on digital computer technology to meet national security demands. One area of increasing concern is use of PDAs, which include everything with a microprocessor and nonvolatile (semi-permanent) memory. Rather than trying to discuss requirements of a multitude of digital devices, this article shows how the emerging technology of personal

digital assistants creates new risks to defense information and networks. Finally, it discusses security policies created to reduce the chance of compromised information or networks from the use of these new devices.

Every time technology takes one step forward, security seems to take a step backwards. This applies to PDA devices also. Although you may not own or use a PDA, you most likely know or will come in contact with somebody who does. Additionally, many of the same risks exist on other types of digital devices.

With basic knowledge of the information in this article, you may be able to prevent detrimental impacts to government information systems. One of the biggest threats facing the Air Force involving PDAs is the possible compromise of information

See **RISKS** next page

RISKS

From previous page

placed on or transmitted by PDAs.

For anyone who is not familiar with PDAs, they include Palm Pilots, Blackberry devices and other small personal productivity computers. Sensitive information placed on a PDA is at risk because there has been no sanctioned procedure to remove classified or sensitive information inadvertently placed on these devices. Additionally, to allow a PDA using infrared or radio signals to synchronize with computer workstations across a network, certain firewall ports must be opened and passwords may be sent in the clear. This increases risks that hackers may gain access to the device or even the entire network.

If you have ever used a computer to connect to the Internet, you probably already know that any device (including PDAs) that can connect to the Internet is subject to several serious risks. First of all, countless eyes can examine any information that crosses the Internet without encryption. If the owner of a PDA uses a commercial Internet Service Provider to transmit official information, the owner exposes the transmitted information to unnecessary risk from hostile entities or intelligence services.

Additionally, any device that can link to the Internet may be subject to hostile actions from other users connected to the Internet. Hostile actions may include espionage, or transferring information or viruses to the PDA. Keeping in mind some of the risks brought about by digital productivity devices, the Air Force has implemented policy measures to minimize potential threats.

It is paramount to establish policy and practices to minimize the risks associated with PDAs because in a networked environment, "a risk accepted by one is a risk imposed on all." In the light of known threats to PDAs, users need to be aware of current Air Force policy published in interim changes to AFI 33-202 (Computer Security) dated June 2. See paragraph 3.5 for additional information.

Because there is no way to purge classified information from PDA equipment, Air Force policy prohibits processing classified information using these productivity devices. Whether you use personal or government-owned PDAs, be aware any PDA that is contaminated with classified information must be confiscated, protected and most likely destroyed. To prevent transmitting official information insecurely, the interim



Photo by Tech. Sgt. Mike Leonard

1st Lt. Ben Cook, Air Force Communications Agency, checks his e-mail using a Palm Pilot.

changes prohibit synchronizing files or devices across a network because of the network configuration changes that would be required.

Air Force policy also clearly prohibits the use of commercial ISPs for conducting official business. Modems on PDAs used for official business can only be used to dial official remote access servers. If followed religiously, these policies will reduce likelihood of hostile actions affecting your PDA or the network.

To follow up on this review of threats and policy-directed countermeasures for PDAs, it's important to apply the countermeasures and watch for others who may unknowingly violate the security requirements. Whether you own or use a PDA or not, many of the same threats and countermeasures apply to other forms of digital computer equipment.

Remember, if you accept a risk with equipment connected to a network, you are also risking the security of all other equipment connected to the network. As the Air Force embarks on the third month of Information Assurance Awareness Campaign 2001, it's important to practice sound security principles every day.

Even though you are constantly deluged with Information Assurance and Computer Security information, it's still important for all government network users to review and heed the guidance. After all, consider how long it might take to recover important files on your computer workstation if you lost them through someone else's failure to apply required security countermeasures.

Viruses affect personal digital assistants and networks

By Master Sgt. John Middleton
*Air Mobility Command
Scott AFB, Ill.*

The threat posed by computer viruses is hardly late breaking news to computer users. Many people learned about them the hard way after the “Melissa” and “I Love You” viruses overwhelmed e-mail systems worldwide, causing damage estimated in billions of dollars. Now people know. However, in the world of computer technology, new threats tend to stay one step ahead of user awareness.

Much attention is now given to the security of networks, desktops and laptops. Far less consideration is given to personal digital assistants such as Palm VIs or Blackberries. No doubt this is partly due to the fact PDAs are used far less than standard PCs. Yet these increasingly commonplace devices are vulnerable. They will become even more so as they increase in sophistication.

Descriptions of PDA viruses used in this article were obtained from the official Symantec and McAfee anti-virus Web sites.

Ironically, the relatively limited capability of current PDA models provides a degree of protection from virus infection. For example, inability to transfer attachments protects most PDAs from one common source of viral infection. This doesn't mean PDAs are immune. In fact, there have already been reports of viruses and Trojan Horse (Trojan) programs designed to attack the Palm operating system.

“LibertyCrack” is a Trojan aimed at PDAs that can be transferred from a host computer during synchronization. When LibertyCrack activates, it attempts to delete applications from the PDA and reboot.

“Vapor” is another Trojan. This malicious logic causes icons to disappear from PDA screens as if deleted, though in reality they are not.

“Phage” is a PDA virus that infects applications, filling the screen with a dark gray box and causing active applications to close. Although experts consider the current risk to PDAs to be low, both the capabilities and the uses of these hand-held devices will con-

tinue to grow. With this growth, the likelihood of a PDA downloading viruses and becoming infected will increase. Of course, viruses downloaded to a PDA from any source could also be uploaded to infect entire networks.

PDA users can protect both personal and official information by following rules that already apply to their desktops and laptops. Don't download program files or macros from any unknown, non-trusted source. These programs and macros may include, but are not limited to, freeware and shareware. Remember not to download freeware and shareware files without prior written authorization from the network Designated Approval Authority.

Use government information technology resources for official government use only. This can't be repeated too often, because one common vehicle for propagating malicious logic is to hide viruses within computer games. Theoretically, Air Force systems should never be infected this way. However, in the security arena, theory is always dependent upon compliance.

Current, properly configured anti-virus software must be in use on all Air Force desktops and laptops. This will provide some protection whenever you synchronize between your PDA and PC. Vendors are beginning to release anti-virus software specifically for PDAs. At some point after evaluation and ap-

proval, these may be used by the Air Force. In the meantime, immediately scanning your hard drive after uploading from a PDA is a must! As with other types of computers, report any suspected PDA virus immediately.

With the usefulness of PDAs expanding, their popularity will probably keep pace. Increased use of PDAs will likely increase the risk of viral infection involving hand-held devices. This risk will be mitigated only to the degree PDA users practice security. Too often in the past, meaningful security efforts have been reactive as a result of major incidents, rather than proactive. With regard to PDAs, we have a good chance to change that by starting early to address potential risks. Awareness of the PDA virus threat is the first step.



The Blackberry is a personal digital assistant.

Protecting and accounting for personal digital assistants

By Renee Osuma
Computer Systems Squadron
Air Mobility Command
Scott AFB, Ill.

Handheld computers are everywhere. Commonly referred to as personal digital assistants, they are slick-looking portable devices you may have noticed your co-workers using to complete their daily tasks, like writing e-mails, taking notes and saving information.

Experts predict that by 2003 there will be approximately one billion wireless handheld computers and smart phones. Furthermore, it's anticipated approximately 600 million will be connected to the Web. Based on these predictions, connections to the Air Force information enterprise will become more common, as PDAs become more readily available to the general public. Consequently, handheld security is an increasingly important issue to Air Force networks.

PDAs and smart phones are uniquely different from laptops and other computers because of their wireless transmit-and-receive capabilities. They often carry sensitive unclassified information and can easily be misplaced. For example, an innocent user carrying important information on a PDA might accidentally leave a device in an airport while on TDY, without having set up sufficient password protection to block malicious use. So how do you keep these devices and their data from getting into the wrong hands? **Guard them carefully and secure them!**

Other concerns might include a disgruntled employee secretly synchronizing malicious data between handheld devices, or downloading sensitive data and releasing it to an unauthorized recipient. This is possible because some devices are so small they are easy to hide and can send data packets wirelessly by radio signal or using an infrared port. This introduces new threats that are difficult to detect or stop.

Because PDAs are increasingly being used to send and receive official e-mail and are used to synchronize

data with networked computers, AFI 33-202, paragraph 3.5.3, requires PDAs meet the same basic security requirements as any desktop or notebook computer. It prohibits use of a PDA for processing classified information and for over-the-air retrieval of e-mail from a commercial Internet Service Provider.

Another Air Force instruction that applies to PDAs is AFI 33-112. Because PDAs have a central processing unit, paragraph 22.1.1 includes handheld computers in the requirement for tracking within the Information Processing Management System. IPMS requirements apply to PDAs even though many PDA units don't meet the minimum cost criteria. IPMS tracking of PDAs ensures computer security Certification and Accreditation is accomplished. Whenever a PDA is lost, a report of survey must be accomplished in accordance with AFMAN 23-220.

Since these devices impose serious risks to networks, Air Force personnel need to take steps to ensure they're properly secured. Here are a few safety precautions for using handheld devices:

- * Use only Designated Approval Authority authorized devices to process official information or to synchronize with a government network.

- * Track accountability of devices in accordance with AFI 33-112.

- * Immediately establish local policy when needed to increase security or accountability standards.

- * Educate users on applicable local and Air Force policies.

- * While TDY, secure and protect devices from loss and theft.

- * Follow Air Force standards for password creation and encryption when devices are used on a network—especially wireless networks.

- * Change your passwords often.

Remember, every precaution you take to protect a PDA also helps protect our networks.



The Palm Pilot Vx is a personal digital assistant.

Digital copiers: intelligent peripherals that pose a significant threat

By Senior Master Sgt. Alan McClellan
*Air Mobility Command
Scott AFB, Ill.*

Imagine sending sensitive information to your networked printer and later finding that because the printer was improperly configured, your files were covertly redirected to an enemy's networked printer. You

might be surprised to learn that networked printers are not the only covert risk to Air Force networks and users. Any intelligent peripheral, containing a central processor and non-volatile memory, and requiring an Internet Protocol address, becomes accessible to hackers whenever strict configuration rules are not followed. You might be more surprised to learn that new digital copiers have many of the same vulnerabilities as networked printers, and have even surpassed the list of known threats to networked printers.

Many offices have replaced older photocopy machines with newer digital copiers and people quickly notice there are network connection ports on the new digital copiers.

Although connecting copiers to the network may sound like a good idea to increase productivity, after reading this article you will understand why digital copiers pose a significant threat to Air Force networks and can't be connected to a government network without extensive preparation.

Many digital photocopiers have all the capabilities of a network computer, network printer, network scanner and network fax machine — all rolled into one. Not only can networked digital copiers accept input from a networked computer for printing, but they can also fax or e-mail numerous copies of any document to any corner of the globe. As a result of these unique features, you need to assess security for digital copiers just as you would for any other server or workstation in your organization.

This article will outline known threats associated with networked digital copiers, discuss available countermeasures to reduce risks, and examine developing policy regarding the use of these devices.

There are several significant security risks associated with connecting digital copiers to your networks.

First, a significant risk exists on a popular model of digital copier, where the key operator code (equivalent to a network server console password) defaults to "00000." This password can be accessed in person, over the network or through a



Photo by Tech. Sgt. Mike Leonard

Staff Sgt. Deshan D. Woods, 375th Communications Squadron graphic illustrator, runs a diagnostic check on the Canon v30 Color Pass System at Scott AFB, Ill. The Canon v30 provides network capability for their laser copier.

dial-up modem. So unless the default password is changed, a hacker might be able to quickly access configuration settings and commandeer copier output.

Second, there are additional risks when default copier GUEST accounts can't be disabled, and where the copier system administrator account name and password are the same. Unseen people can exploit these weaknesses from remote locations, changing IP settings or enabling any of the several less secure communications protocols available on digital copiers.

Third, networked copiers introduce new risks of outsiders halting network operations by flooding digital copiers with File Transfer Protocol print requests. Consider how easy flooding the network might be when a popular model of digital copier allows anonymous print requests when submitted by a user named "PORT1."

Fourth, an intruder who is able to control a new digital copier might be able to control other networked printers, because some digital copiers use standard PUBLIC and PRIVATE Standard Network Management Protocol community strings, and fail to provide guidance or any utility to change the SNMP default settings. Imagine having somebody redirect output from any unprotected base printer after capturing control of a single networked copier.

Fifth, some digital copiers can be managed remotely through an embedded Web server function that can be accessed using the copier IP address as the Web Uniform Resource Locator. Through HTTP, anyone can view image counts and enable the fax-to-file and fax-to-e-mail options if you have the network scanner option installed. Additionally, passwords are not required in the default setting to access Web-based copier management functions.

Sixth, the most recent documents processed on most digital copiers are stored on hard disk and can be accessed by anyone using a "demand reprint" function, posing a risk to sensitive information.

And finally, even if a digital copier is configured as securely as possible, copier technicians are usually not experts in network security, and may inadvertently disable security parameters and fail to reset them. This is a significant threat because most people don't pay constant attention to the copier technicians. With these risks in mind, you need to be aware of some possible countermeasures. Use the following checklist as a guide to minimize security risks, if your Designated Approval Authority authorizes a digital copier for your base network:

- * Prepare a Certification and Accreditation package.
- * Change the default Key Operator codes and administration passwords, to protect your secure configuration and ensure passwords meet Air Force standards.
- * Enable secure passwords for HTTP management

that meet Air Force standards (minimum length, password longevity, etc.).

- * Change the default Public and Private SNMP community strings, or provide countermeasures to minimize threats.

- * Verify what copier services are running, to help determine whether features need to be turned off or which settings need to be changed.

- * To minimize potential risks, disable all unused features and network protocols.

- * If remote management through a modem is used, ensure the modem is disabled when connected to the network.

- * Disable the demand reprint function. This prevents unknown persons from retrieving copies of documents previously processed.

- * Disable e-mail relay options, to prevent intruders from passing your documents to unauthorized recipients.

- * Consider routing all networked copier problems through computer system security officers or workgroup managers, to verify that security settings retain integrity.

- * Consider using the CSSO or WM to verify security configuration each month.

- * Verify credentials and validity of service calls each time copier technicians are given access to networked copiers. Check to ensure all security settings are correct after they leave.

- * Find out what embedded management package is being used and check for vulnerabilities.

- * Consider using a copier or printer control system. This provides an audit trail of who used the copier and when. They can be used in client situations for cost recovery.

- * Scrub the copier when you dispose of it. The hard drive may still have a buffered image of the last document that could be retrieved if the hard drive was pulled out of the unit.

This list is not all-inclusive because new features are continually added; however, it provides some advice for correcting many known deficiencies of networked copiers.

Hopefully this article has convinced you that these new multipurpose digital copiers require more than a "plug-and-play" attitude. To ensure you have taken all necessary measures to secure your network from threats, you must complete a C&A package according to AFSSI-5024, and receive approval from the network DAA before connecting a digital copier to an official network. Even after completing the C&A, security configurations must be checked and rechecked continuously if you wish to prevent your print output from being diverted to an unknown hacker's printer.

IA awareness, training and education: Do you know the differences?

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

Most people don't make a clear distinction between awareness, training and education. But the desired outcome of each is different. Awareness heightens the importance of a subject and points out possible consequences if people don't apply the prescribed policies and procedures. In regard to Information Assurance awareness, it's necessary to explain what can happen to an organization, its mission and users if they fail to take security seriously.

Information Assurance training is more specialized and is tailored to a particular job. Anyone requiring access to the network needs to be licensed. Licensing requirements are outlined in AFI 33-115, Volume II, *Licensing Network Users and Certifying Network Professionals*. In a training environment, the student actively participates and acquires new insights, knowledge and skills. Education includes the type of in-depth training available from a technical school or a college course.

So, why does the Air Force need Information Assurance Awareness Campaign 2001? Because the Air Force needs to continuously stress the importance of maintaining Information Assurance at all levels. It's more likely for someone to remember something if they

receive pieces of information throughout the year, rather than all in one month. Awareness can be made useful by addressing security issues that directly affect the users. The goal is to improve basic security practices, not to make everyone literate in all the jargon or philosophy of Information Assurance.

For example, when there's a change in network security policy, users can be notified with an e-mail message. Then, you can point them to Intranet, a Web page, or a hard drive where the entire policy can be found and reviewed. If you point out the small changes, rather than requiring people to read the entire policy to find them, users will be more receptive and better informed.

Effective awareness programs are designed on the premise that people tend to undergo a "tuning out" process. When was the last time someone stopped to look at the bulletin board they walk by every day? Maybe someone hung a new poster and people stopped just long enough to read it. But after awhile, no matter how well designed, the poster will be ignored. It will, in effect, simply blend into the environment. For this reason, effective awareness techniques require creativity and frequent change.

Changing the mindset of users doesn't happen overnight. Ideally, it's a continuous process that someday will help to make Information Assurance in the Air Force a day-to-day practice.

Use of Personal Digital Assistants

DOs:

- Process unclassified information from desktop--
 - * schedules
 - * contact info
 - * notes
 - * e-mail
 - * other Outlook items
- Take notes, save info, or write e-mails while away from desktop
- Synchronize info back into your desktop



DON'Ts:

- Process/maintain classified information
- Connect/subscribe to commercial ISPs for official e-mail services (e.g., Palmnet Wireless Communications Service)
- Synchronize files or devices across the network via wireless connections
- Arbitrarily download and load freeware or shareware software enhancements

PDA Modem Use:

Only authorized connection is to an official AF RAS account protected by an authorized NCC firewall

Desktops will NOT be configured to permit direct dial-in access for the purpose of synchronizing the PDA remotely

Carl von Clausewitz on information in war: a matter of trust

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

Prussian Gen. Carl von Clausewitz (1780-1831), foremost military scholar of the Revolutionary and Napoleonic war period, emphasized the critical nature of information in warfare in his book *On War* in 1832. He asserted that information, along with ideas and actions, form a “foundation.” He said, “*Let us just consider the nature of this foundation, its want of trustworthiness, its changefulness, and we shall soon feel what a dangerous edifice War is, how easily it may fall to pieces and bury us in its ruins.*”

The general further emphasized that the inability to know what ground truth is adds great friction, saying, “*This difficulty of seeing things correctly, which is one of the greatest sources of friction in War, makes things appear quite different from what was expected.*” General Clausewitz strongly believed that accurate and timely information was a very critical factor in war.

Today these words hold even greater importance to us because we have rapidly transitioned into an Information Age. Keeping our networks and information systems secure and reliable is a formidable task. The term Information Assurance itself quite literally emphasizes our dedication to reducing the *untrustworthy* and *changeful* nature of information as much as possible. Many of the physical security measures we take are intended to ensure information systems are reliable and trustworthy. In the corporate information technology world, however, physical security often plays a minor to nearly non-existent role ... which leads to this next point.

One of the key differences between our Department of Defense information infrastructure and the Internet, corporate networks, and other information systems is that we take our systems to war with us. This is a far more complex challenge that dramatically sets us apart from average corporate America. Most physical security references for the protection of computer systems include a standard list of potential threats and hazards, such as:

- * weather and internal climate (storms, smoke, temperature, humidity, etc.)
- * natural disasters
- * fire/water/electrical hazards
- * building structure (age, windows, walls, ceilings, floors)
- * disgruntled insider or former employee, and
- * hackers, crackers, vandals, criminals.

A problem in any of these areas can adversely affect the performance and reliability of systems, and hence not only whether through our systems we “see things correctly,” but also whether our systems are available so we can see anything at all. Additionally, we must:

- * learn our enemy’s military and political information policies and strategies,
- * deploy and secure our systems during war and contingencies, and
- * expect greater numbers and types of hostile information system attacks.

This overwhelming task requires everyone on the Air Force team to be fully engaged in Information Assurance daily. One person’s lapse in good password discipline, inattention to harmful changes in a system’s physical environment (e.g., fire, water, electrical, etc.), or careless practice causing a denial of service from within our ranks can introduce fog and friction that would cause even General Clausewitz to blink.

This month’s Information Assurance Awareness Campaign theme is *Digital Devices* and is hosted by Air Mobility Command. While digital devices take us a step further into the Information Age and increase our information system value and utility, they also present new physical security challenges. Small digital devices are more easily stolen or lost, and therefore require more positive physical controls. Digital devices may also require additional internal safeguards to prevent system compromise.

As a final reminder, each Air Force team member is obligated to practice and promote effective Information Assurance ... to provide leadership and command authorities with information they continue to trust ... so they may “*see things correctly.*”

AF Enterprise Directory Services: powering the network

By Wing Commander Andy Powell
Royal Air Force Exchange Officer
Office of the Air Force Deputy Chief of Staff
for Communications and Information
Washington

In the near future, you'll be able to go to any Air Force terminal and, with nothing more than your new Air Force ID, log into the Air Force network. The Air Force Portal, tailored to your role and personal preferences, will appear. You'll have access to a huge variety of network resources and applications and, with few isolated exceptions, you'll need no additional user IDs or passwords. You will no longer have to re-enter your personal information at numerous locations as you make a PCS move, and the information you need will be available and accurate from the designated authoritative source.

The complete network will be managed and configured from a small number of remote locations where, through a controlled but simple set of key changes, it will be possible to change individual or group access permissions to network services. This seeming "Nirvana" is known as a "shippable place" in the IT world, but to the user this level of service will be essential in a network-centric Air Force. Without Directory Services, none of this could happen!

A number of projects are delivering the tools to meet this vision, but the essential services needed to support all of these projects are part of the Air Force Directory

Services. While on the surface this may not seem to be the most exciting project, Directory Services is really akin to the legs of a duck paddling furiously under water.

The Air Force Directory Services Focus Group was formed in October to expand upon the successful initial Directory work started in July. The initial Directory Group efforts delivered the Air Force "White Pages"

that for the first time provided a single focal point for finding key information on Air Force personnel. White Pages was the result of excellent teamwork between a number of agencies, including Air Force Personnel Center and Electronic Systems Center's Systems Support Group, and was successfully demonstrated at Corona Fall. It has subsequently been integrated as an essential application on the Air Force Portal.

However, Air Force Directory Services is more than White Pages, and the direction given to the expanded group in October was to establish "an Enterprise-wide Directory Service able to provide secure, timely control and access to all resources required of a network-centric Air Force."

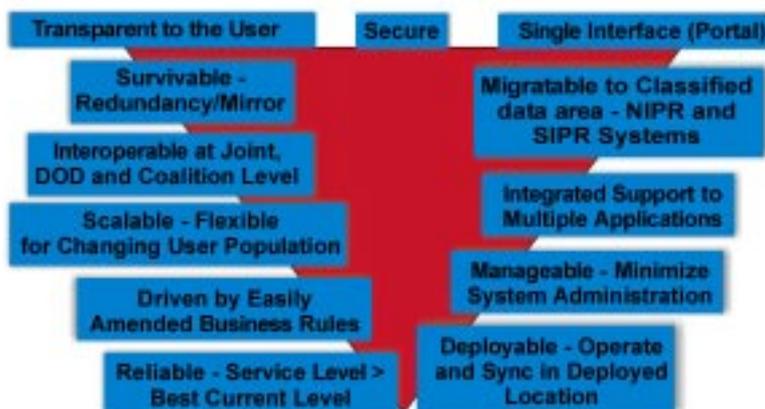
In short, it was to be "an honest broker – a third party that directs users to authoritative data." The group is led by Wing Commander Andy Powell, a Royal Air Force Exchange Officer, working for Lt. Gen. John L. Woodward Jr., the Air Force Deputy Chief of Staff for Communications and Information.

The group includes a wide range of representatives from the major commands and agencies, but its challenge is highlighted by the number of team members from existing Air Force projects that rely heavily on the provision of an Air Force Enterprise Directory Service.



Graphic by Staff Sgt.
 Jason T. Arnold

Air Force Directory Services - Goals



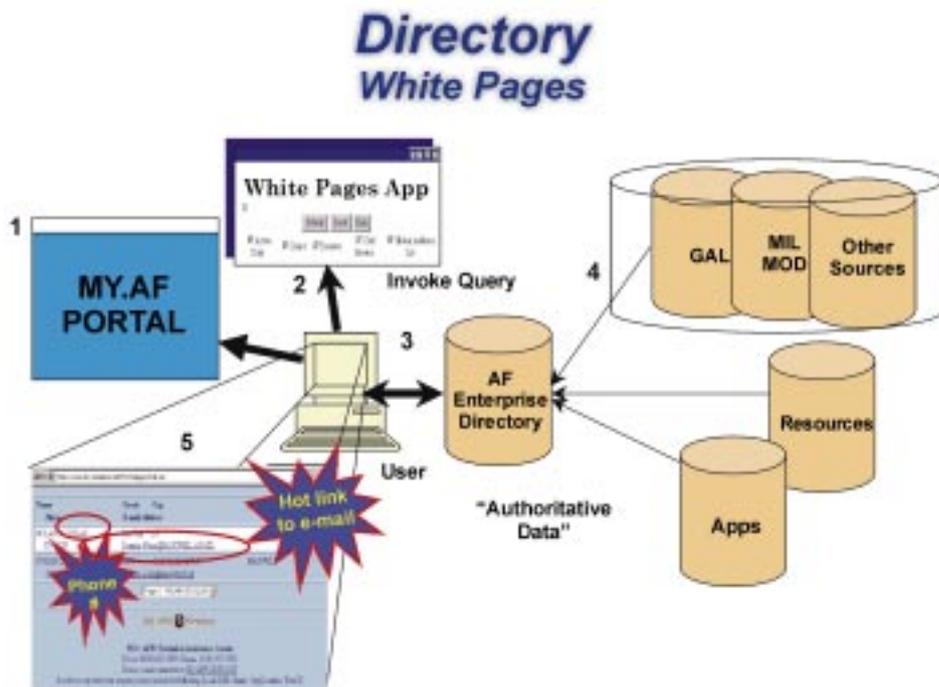
The Air Force Public Key Infrastructure and Common Access Card will deliver authentication to the network, with Windows 2000/Active Directory providing the tools to manage all the network resources and common services, and the Global Combat Support System – Air Force delivering access to mission support applications as required. All are reliant upon the provision of an Enterprise Directory Services structure.

The challenge to the group is significant and the aim is to build a pilot Air Force Directory Services by June 30 to bridge the developing GCSS-AF and Windows 2000 communities, and to then expand within the communities and across other areas such as Global Directory Service, PKI and CAC. The growth of the Directory Services provides the flexibility and remote management tools that are also absolutely essential to the Air Force's initiative to consolidate servers. This has already been successfully demonstrated by Air Mobility Command's E-mail Consolidation pilot at Charleston AFB, S.C., that relied heavily on integration of a successful directory service. There have also been great strides in building an enterprise "container" for network users and developing a common method of uniquely

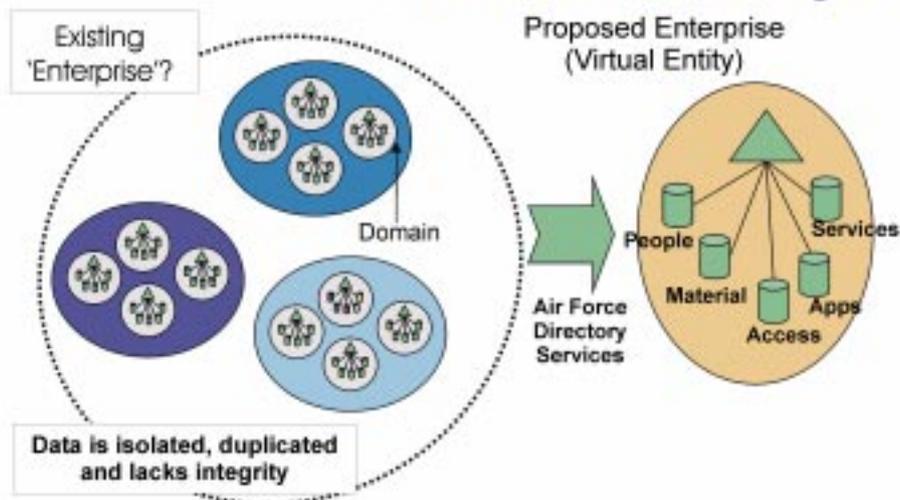
naming network resources to allow them to be more widely shared.

As the Air Force moves increasingly toward network-centric operations, robust and powerful Air Force Enterprise Directory Services will be the unseen but essential ingredient.

For more information, please contact Wing Commander Andy Powell, HQ USAF/SCTA, at DSN 425-6179, or (703) 588-6179.



Directory Services More than Just 'White Pages'!



Senior communicators formulate direction of AF IT Enterprise

By Maj. Jodine K. Tooke
*Deputy Director,
Director's Action Group
Air Force Deputy
Chief of Staff
for Communications
and Information
Washington*

Air Force and Defense Information Systems Agency senior communicators met at the Server Consolidation Summit at the Air National Guard Readiness Center, Andrews AFB, Md., Feb. 1-2. The summit marked an important milestone in the progress toward achieving the goals outlined by Secretary of the Air Force and Air Force Chief of Staff in two policy letters released in early January.

The summit's main objective was to formulate future direction for the Air Force Information Technology Enterprise, specifically for security, server consolidation and communications and transport architecture. The summit also gave participants an opportunity to address cross-cutting communications and information issues, such as resource use and how to address tenants and geographically separated units.

The conference identified the need to migrate to an Air Force "Community of Interest" Intranet, much like most large commercial enterprises, but with greater emphasis on

warfighting support and security. Conferees recognized that, as the Air Force moves forward with initiatives such as server consolidation and My.AF (the Air Force Portal), information pathways must improve in terms of security, reliability, manageability and throughput. However, much work lies ahead to turn the proposals into reality.

All major command directors of communications and information, and the Air Force Pentagon Communications Agency commander, briefed their server consolidation progress and plans, providing insights on their desired end-states, objectives and benefits, metrics, road map, recent actions and accomplishments, way ahead, challenges and issues, and take-aways. Attendees shared lessons learned and benefited from discussions that brought everyone to a new level of understanding.

Lt. Gen. John L. Woodward Jr., Air Force Deputy Chief of Staff for Communications and Information, concluded the conference by asking participants to leave fully engaged, as full partners in creating one Air Force enterprise. Conferees left with a stronger commitment to creating a single Air Force enterprise, a clearer picture of the way ahead for consolidation, and a common understanding of the security architecture.

DMS Web page provides new functionality

SCOTT AFB, Ill. — If you're a Defense Message System user, administrator or program manager, finding information on the Web just got easier. Air Force Communications Agency's DMS Field Support Branch has completed a renovation of the Air Force DMS Web site creating a functional, easy-to-use information source.

Upon visiting the Web page, the first thing you'll notice is the choice of profiles available to you. Once you select a profile, all the links for information related to that profile are displayed. For example, if you're responsible for preparing organizational messages for your unit, then you'll choose the End User profile and be directed to documents and information relating to end users only. If you're a program manager, there's a profile with pointers to information of interest to you, but not necessarily an end user. The profiles help reduce the amount of time needed to search for information.

Visitors to the site are not restricted to any particular profile. If you're a system administrator and would like to use the Program Manager profile, then help yourself. These profiles are intended to help you go directly to the documents and information you most likely will need to accomplish your job. The new profiles have been created not to restrict your access, but to expedite your access to the information you need most.

The new profiles aren't the only change. The look of the page has been revised and a couple of topic views have been added to help narrow your search.

More changes are forthcoming. Currently AFCA and Standard Systems Group at Maxwell AFB, Gunter Annex, Ala., maintain separate DMS Web sites. A plan to merge the sites is under way to establish "one stop shopping" for DMS. Comments or suggestions for improving the site can be directed to afca.itif@scott.af.mil, DSN 576-5351 or (618) 256-5351.

Dynamic Network Analysis toolkit automates network planning and analysis functions

By **Kenneth McIntyre**
*Architecture and Interoperability Directorate
Air Force Communications Agency
Scott AFB, Ill.*

The Air Force Communications Agency's Architecture and Interoperability Directorate is building a computer-based toolkit designed to automate network design, modeling and performance analysis for communications planners and network managers. The Architecture Development Branch, led by Maj. Mark Thompson, has the difficult task of integrating several commercial off-the-shelf application programs into a fully functional and portable toolkit. Network

performance is fundamental to the day-to-day operation of an Air Force base. The Dynamic Network Analysis toolkit will be a powerful resource for helping network planners build and manage high-performance networks and observe service levels to support their needs.

The DNA toolkit will generate a comprehensive computer model of a base's existing local area network, and give the capability to project the impact of new applications, technologies and traffic patterns on network performance. Planners will have the ability to simulate and test various solutions for maintaining desired service levels, and run any number of "what if" scenarios to test different options and aid capacity planning. Network upgrades and configuration changes can be simulated to save time and money prior to actual purchase and deployment.

DNA toolkit integrates several COTS network modeling and network monitoring software products into a complete network mapping and scenario simulation package. The toolkit creates interactive network maps with click-through details on each network device and performance-level graphics illustrating the impact of changes on the network.

The toolkit consists of three primary components:



Photo by Master Sgt. Ed Ferguson

Kenneth McIntyre, Dynamic Network Analysis systems engineer, gets clarification on a network device model of a Cisco Catalyst Switch from its creator, Thao McLeland, DNA lead engineer.

Core Network Modeling and Simulation Software

OPNET Modeler was selected for the toolkit to provide modeling, simulation, traffic analysis and predictive capabilities. It allows the network administrator to design and study communications networks, devices, protocols and applications and create "what if" scenarios for predicting the impact of change on the network. It complements network management and measurement tools by enabling proactive decision making. It creates graphic displays of network performance levels, and optionally has the ability to graph projected service levels achieved through alternative courses of action in a virtual network environment.

Modeler's object-oriented modeling approach and graphical editors mirror the structure of actual networks and network components, so models intuitively map to their systems.

Additional analytical network analysis software (e.g., NetRule, NetMaker) are under evaluation. Whereas OPNET 7.0 uses discrete-event analysis (virtually every event is simulated), an analytical network

See **ANALYSIS** Page 21

Air Force enters new era with portal

By Chuck Paone
Electronic Systems Center
Public Affairs
Hanscom AFB, Mass.

Far more than just another Web site, the Air Force Portal, soon to be introduced by the Electronic Systems Center here, will ultimately change the way nearly all Air Force people and employees work.

The idea, according to Lt. Col. Kevin Erickson, Air Force Portal program manager, is to give people instant, desktop access to all the information they need to do their job. Rather than simply connecting by links to sites that offer limited, fixed information, workers will be able to enter content areas and work with information on line.

"This new portal, when fully implemented, will provide a single point of access to the right information, at the right time, in the right format, and from any location," said Lt. Gen. Leslie Kenne, ESC commander. "It's exactly the kind of tool we need to help our Air Force maintain the competitive edge."

The portal will give people access to the entire Air Force database from their desktop. Access will be granted on the basis of functional need, and will ultimately be available from a single log-on.

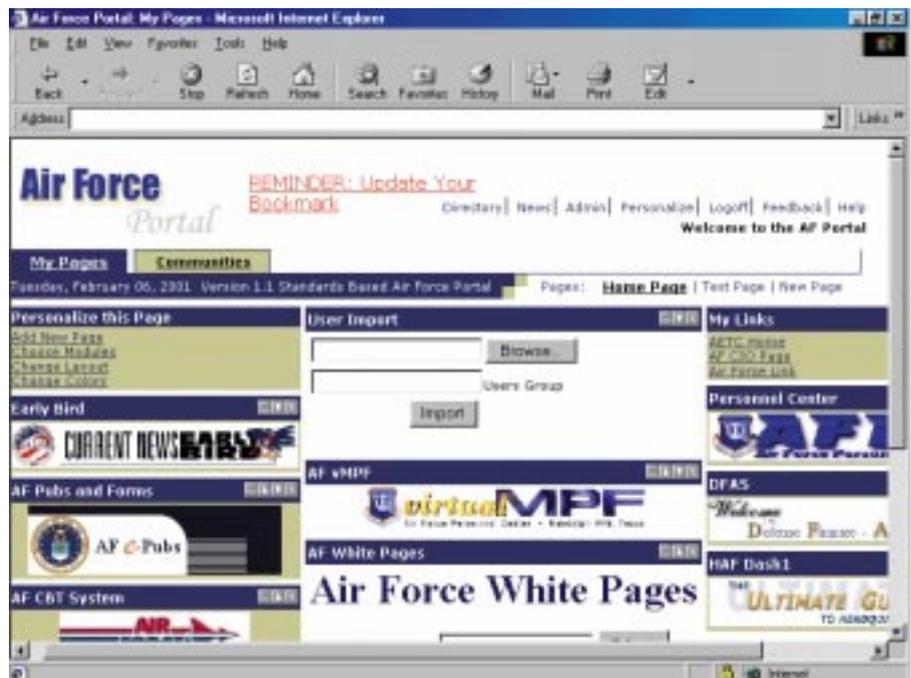
"The system will recognize you when you log on and will know what access you're entitled to," Colonel Erickson said. "That means you'll no longer have to keep different log-on user names and passwords for every new content area you need to enter."

MITRE, a federally funded research organization, is providing engineering and design support for the portal.

The new Air Force Portal will reside on the Air Force's Global Combat Support System integration framework, said Tom Gannon, MITRE information systems engineering director. This will provide the commonality that affords access to vital Air Force information, he said.

Initial features will include access within the Air Force to information systems for inventory management, maintenance, medical, personnel, computer-based training, communications, finance, acquisition, contracts, transportation, warrior and frontline combat.

Each user will be able to customize and personal-



A look at a My.AF desktop screen with some of the options available to Air Force members. The service's goal is to quickly move into a new technological age by providing a My.AF account to every Air Force member by July.

ize his or her view into the wide range of information, Gannon said.

The portal is designed to disseminate information for peacetime and wartime communications rapidly, said Dennis Volpe, ESC Information Programs Office director.

"This will give warfighters more timely data, which they can use to plan their combat missions," he said.

Even when not being used for direct combat support, the portal will still be primarily a warfighter support tool, Volpe said.

"ESC is responsible for acquisition of command and control tools needed for combat support, and this portal will allow us to do that more efficiently," he said.

The portal will be based on open industry standards and use an architecture developed by MITRE that allows the software to run successfully on multiple computer hardware and operating systems. This will afford the instant compatibility needed to ensure all Air Force users are able to benefit from the system, and will allow flexibility to incorporate new technology as it becomes available.

The greatest challenge in fielding the portal will be creating interfaces with more than 700 Air Force legacy databases, Colonel Erickson said.

See **PORTAL** next page

ANALYSIS

From Page 19

analysis tool makes generalizations that allow simulations to run in a fraction of the time. As these and other new network analysis software prove their value, they will be added to the DNA toolkit.

Network Topology

To rapidly represent base networks, HP OpenView Network Node Manager (available as part of Combat Information Transport System Phase II) was selected to provide network topology for import into OPNET. Network discovery, documentation and design capabilities are enabled through NNM. NNM provides concise and in-depth views of network devices and their status in an intuitive graphical format. In addition, NNM discovers network devices and provides a map to illustrate what the network actually looks like. The multi-level map indicates which devices and network segments are healthy and which areas need attention.

Network Data Traffic

Key to effective modeling and simulation is gathering actual traffic data traveling across the network.

To quickly size up the use of links and nodes without installing hardware probes, Concord eHealth will be used to provide rapid utilization levels. This is extremely valuable for "what-if" scenarios, where additional load will be simulated on already-encumbered network links to evaluate the impact.

For more accurate network data traffic analysis, a suite of Agilent Technologies, Inc., hardware probes are part of the toolkit, including Ether, Fast Ether, Gigabit Ether, and ATM. Agilent's NetMetrix software was selected to gather the probe's network traffic data and facilitate import into OPNET. The NetMetrix library of network devices supports the mapping of ex-

isting networks in minutes, including click-through configuration and option details on network devices from all major manufacturers. The software also supports design, and validates interoperability of devices.

Project Status

Using a representation of a typical base network in AFCA's Technology Integration Facility, AFCA's Architecture Development Branch – with assistance from AFCA's Technology Directorate and Global Connectivity Directorate, and Air Mobility Command – has successfully tested a prototype version of the toolkit. The lab's representation of topology was imported, FastEther and ATM probes were installed, and actual traffic data was imported. Numerous "what-if" simulations were run, testing several scenarios, including the impact of infrastructure changes and the addition of several hundred simulated users and their applications. Optimal configurations and upgrades were determined, proving the worth of simulation of options prior to a base's actual purchase and deployment.

First-time live use of the toolkit is planned at Scott AFB to analyze the impact of e-mail server consolidation on base network performance. AFCA engineers will team with 375th Computer Systems Squadron, 38th Engineering Installation Group systems telecommunications engineering managers, and AMC to collect the base network architecture and traffic flow data using automated software tools and network probes. The network engineers will then import the data into OPNET for analysis.

After completion of modeling and simulation activities at Scott, more bases will be solicited for interest in the DNA toolkit. Additional information is available from Maj. Mark Thompson or Thao McLeland, DSN 576-5448, (618) 256-5448, or by sending an e-mail to afca.ita@scott.af.mil.

PORTAL

From previous page

The portal was designed to access existing databases by using so-called "middleware."

Still, this is no easy task. "For each of those 700 legacy databases, we need a migration plan, and each requires the resources to support the plan," Colonel Erickson said.

Eventually more than one million people will regularly use the new portal. The acquisition and development team for the portal — ESC, MITRE and Lockheed Martin Federal Systems — are testing and evaluating commercial products for scalability and performance, to ensure the portal will be able to meet this demand.

Air Force officials envision that many users will eventually make the portal their home page, where they will accomplish their Web-based work.

"It's hard to imagine all the possibilities for this technology," Volpe said. "But one only has to look back over the past 10 years to see how much things have changed, to see how differently we all work today. This portal is the type of tool that will dramatically change the way we work in the future."

This month, the Air Force plans to unveil a version of the portal that will be available for up to 100,000 selected Air Force users across the major commands. This version will give people a feel for what the portal has to offer and will elicit feedback. Another version, scheduled for release in June, will be available to a wider group of Air Force users, and will have more features, including a powerful new search engine that will quickly retrieve relevant information from a wider variety of sources.

The portal has already been demonstrated and received a positive response from a number of Air Force senior leaders, including Ron Orr, Assistant Deputy Chief of Staff for Installations and Logistics, and John Gilligan, Air Force Deputy Chief Information Officer. (*Air Force Print News*)

Program puts war info at fingertips

By Staff Sgt.

Karin Wickwire

*355th Wing Public Affairs
Davis-Monthan AFB, Ariz.*

Pushing the technology envelope once again, a Davis-Monthan programming team has developed a command and control system that gives warfighters near real-time information critical to their missions.

The Wing Operations Center Network, which grew from the base's Briefing Room Interactive program, made its "very successful" wing debut in December during an operational readiness exercise "trial by fire," according to Lt. Col. Stan Harmon, chief of information technologies for the 355th Operations Support Squadron.

WOC-Net was originally developed to display information — mission-oriented protective postures, alarm conditions and threat conditions — on computer screens around the base. To meet the real-time requirements vital to the warfighting mission, the system was designed to update the information every six seconds, so any computer monitoring WOC-Net had the current information, said Ken Matesich, a programmer with BAE Systems. He got started on the project with the work on Briefing Room Interactive, which began as a tool to automate the mission planning process for pilots.

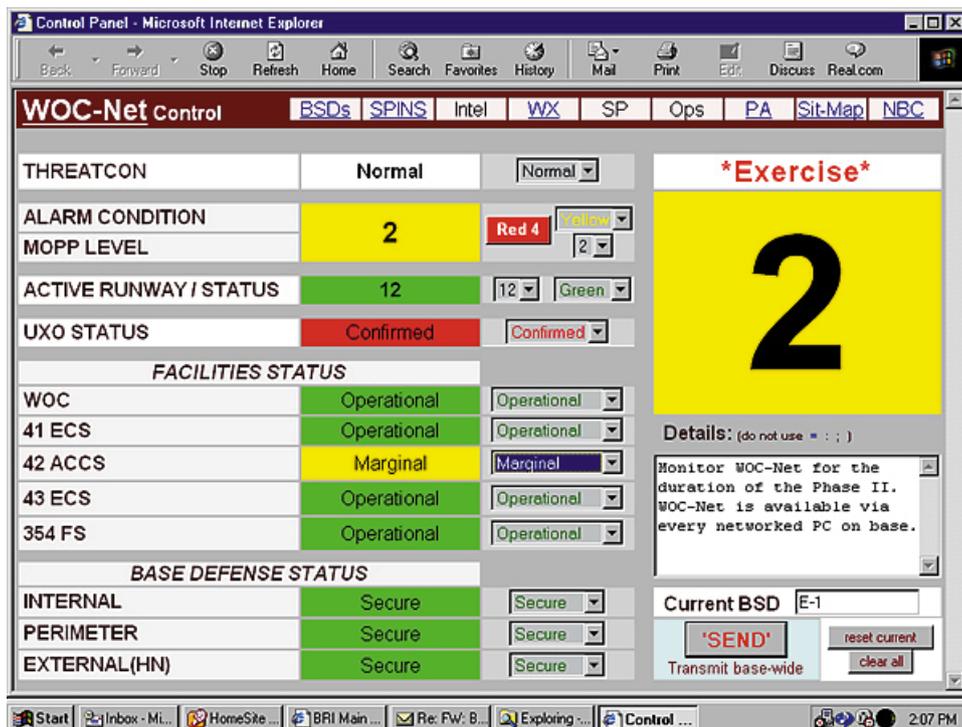
WOC-Net quickly evolved during the exercise, under the pressure of users learning a new system and programmers trying to keep warfighters as informed, and safe, as possible.

"An audio alert and numerous refinements were added to the program during the exercise. We updated the user functionality as they were using it live," Matesich said.

Some of the improvements made after seeing WOC-Net in use focused on the system itself, including color and layout changes to make the WOC-Net control panel easier to read and use, said Sam Furrow, a graphic designer with BAE Systems.

But it was other improvements that mattered most to the warfighters.

"We added direct links to various supporting Web pages, turning the WOC-Net into an effective hub of information," Furrow said. "When the WOC-Net trans-



An example screen seen by users of WOC-Net during an exercise at Davis-Monthan AFB, Ariz.

mitted that a new (battle staff directive) was in effect, people had a direct link to that BSD, as well as links to weather, (special instructions), training, and public affairs sites."

Colonel Harmon said one added WOC-Net tool that really paid off was the Sit-Map, or situational map, which was used to mark the exercise's unexploded ordnance, craters and areas contaminated by chemical or biological weapons.

"This near real-time information can be critical to anyone who would have to negotiate these obstacles to accomplish the mission as quickly and safely as possible," Colonel Harmon said.

Air Force decision dominance over potential enemies was boosted at every echelon of command. WOC-Net's "great command and control capability gave (us) the ability to pass instantaneous and continuous status updates to all wing organizations," said Col. Bobby Wilkes, 355th Wing commander.

"Because of the improved accuracy, timeliness and depth of information, WOC-Net represents a quantum leap in the ability to provide command and control at the tactical and wing levels," said Lt. Col. Guy Walsh, 355th Operations Group deputy commander for A-10s.

Lt. Col. John Sokolsky, 355th Operations Support Squadron commander, shares Colonel Walsh's opinion.

See **FINGERTIPS** next page

AF finance Web site offers 'one-stop' shopping

WASHINGTON (AFPN) — A new Air Force Financial Services Center Web site has everything military and civilian members could possibly want to know about military pay, travel and even personal finance, according to Col. Gregory Morgan, director of accounting, banking and comptroller support.

"The site is designed to provide one-stop shopping on the Web for our customers' financial questions and self-service transactions," Colonel Morgan said.

The site allows people to access, review, and, in a limited fashion, modify personal pay records, including allotments, W-4s, savings bond program participation, and thrift savings plans (for civilians), he said.

"You can also view your latest leave-and-earnings statement or calculate how much that pay raise or promotion will mean to the bottom line," Colonel Morgan said.

To make the site as user-friendly as possible, "We have placed various links on the page to pay tables and allowances, per diem rates, currency converters and more," said Christian Westergard, the site's project manager.

Also on the site is a link to the Employee/Member Self-Service system. Previously, only civilian Air Force employees could access EMSS; however, personal identification numbers were recently mailed to active-duty members allowing them to create a password and log onto EMSS also.

"While members can go directly to EMSS, we believe that by providing that link in addition to a wide



variety of pay, travel and other information, we will provide greater customer value and interest," Colonel Morgan said.

"We have even included a personal finance link that takes you to sites with information about handling your personal finances," Westergard said. "These sites can provide you help with buying a home or a car, or investing strategies."

The concept was based on the idea that with only a mouse click, Air Force members and civilian employees could quickly locate the financial services applicable to their work and personal financial management, Colonel Morgan said.

"This saves our customers time in searching for these resources," Colonel Morgan said. "But, more importantly, it saves them from having to wait in line at the finance customer service window."

The Air Force Financial Services Center Web site can be accessed at <http://www.saffm.hq.af.mil/affsc/>.

FINGERTIPS

From previous page

"The WOC-Net was the most significant wing-level command and control innovation since the creation of the field phone," Colonel Sokolsky said. "As a mission director, I was able to notify every operations center of our ability to survive and operate status within 10 seconds of the senior leadership's decision."

In past exercises, it would take anywhere from 30 minutes to two hours to get that information to the work centers throughout the wing, Colonel Walsh said.

"Now, anyone with D-M intranet access has instant situational awareness of the current MOPP, ThreatCon and alarm conditions. In addition, the text block allows us to pass ungarbled information directly to every leadership level," Colonel Sokolsky said.

That direct information transfer was one increased command and control benefit offered by WOC-Net. A second C2 aspect surfaced when freedom gained from the time consuming notification task meant Colonel Sokolsky, as the mission director, could direct more of his attention to the air war and the strategy for aircraft departure and arrival.

Even though WOC-Net performed better than originally advertised, it's important to note that it was designed as a technology demonstrator and test bed. It isn't a completed project, said Furrow, the graphic designer. "We had an excellent chance to work directly with the users of a new product during that product's creation. With further development, the potential of the WOC-Net is great." (ACC News Service)

Confine contacts with contractors

By Joseph J. Hinds
Air Force Communications Agency
Staff Judge Advocate Office
Scott AFB, Ill.

Don Doe is a government contractor employee who works side-by-side with Fred Fed, an Air Force civilian employee. Don and Fred have worked together in the same office at Flyby AFB for a year and have become personal friends. The two "buds" may appear to be co-workers to an outsider, but they clearly are not. Don certainly is an important member of the team, helping to accomplish the Air Force mission, but there is an established etiquette that must be followed to ensure compliance with federal contract rules. Failure to do this could cause serious problems for both Don's contractor employer and Fred's federal agency.

There may be a tendency for Fred to forget that Don represents a government contractor, since they work together on a daily basis, but Fred must be aware of the rules relating to his contacts with Don. Fred must confine his contacts within a legally defined area. Use your legal office to help you determine the limitations on your contacts with contractors. Change the facts and you change the applications of the law.

For example, Fred may not ask Don to perform special projects that were not contemplated by the contract or to perform out-of-scope work. If Fred sprained his ankle in a softball game, he can't ask Don to go upstairs and get some copy paper for the Xerox machine unless this activity has been included in the contract. There even may be a provision in the contract for Don "to perform other duties as assigned," but this is not sufficient to bring these extra assignments within the scope of the contract. And even if Don doesn't whine while doing all these extra duties, his company can still submit a claim billing the federal government for all of the out-of-scope work. Usually this is done if the contractor does not get its contract renewed.

The next day, Fred, who is cranky because his girlfriend left him, starts supervising Don as if he were the boss. Fred tells Don that from now on, he is going to monitor all of his work and, oh by the way, make a reservation for him to take a trip to the Bahamas so he can use some of his "use-or-lose" leave. This appears to cross the line and become a personal service contract, which is not permitted.

A personal service contract may exist because Don now appears to be a federal employee. In this case, when Fred started exercising constant direct supervision over Don, the contractor was then being treated

like a federal employee. Federal employees normally perform these personal services, unless Congress has authorized these services under contract. Again, the result may be that the contractor can claim reimbursement for these services in addition to its contract fee.

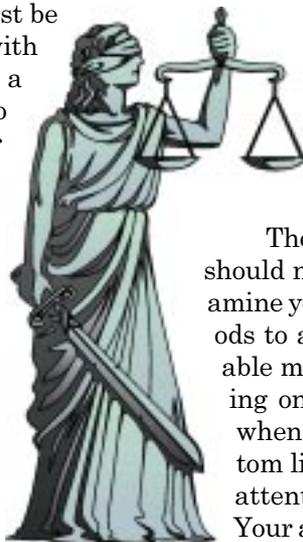
So, what is the downside for Don's company in this hypothetical situation? Don may get so involved with the government that his company becomes ineligible for future contracts in this area. Furthermore, competitors may protest awards on the basis that the winning contractor had communications with the government prior to the proposal that gave it inside information and an unfair advantage over the competitors in the bidding process.

The following week, Fred hears that contractors are receiving letters of appreciation from the Navy, so he wants to send these letters to all his contractors so they will work harder. Many times Air Force employees want to do what sister services or other Air Force members are doing or have done. We have to be careful before proceeding, because it may not be legally appropriate just because somebody else is doing it. The other service may not have asked for a legal opinion, or if it did, the facts of the situation may be different.

The general rule is that letters of appreciation should not be sent to contractors. The JAGs can examine your situation, to help you come up with methods to accomplish your mission in a legally acceptable manner. The legal office might suggest focusing on making timely payments and award fees, when appropriate, to the contractor, since the bottom line with business is profit. You get their full attention when you get near their pocket book. Your appreciation for a job well done might be more favorably received in the form of timely payments and award fees, rather than letters of appreciation. Also, favorable comments on current performance can be given to the Contracting Officer and can be reflected in the Contractor Past Performance report in order to benefit the contractor in obtaining future contracts.

Letters of appreciation are just the tip of the iceberg for issues relating to contacts with contractors. How many times have you heard about a retired officer who is now a contractor visiting his old military friends, letting them know about his company's product? And during the meeting with his former co-workers, he is asking questions about what the Air Force needs and seeking commitments from them to allow his company to "help" the Air Force.

JAGs are available to assist you in working through these difficult contract issues. The first step is the most



DOD launches Web site for transitioning servicemembers

WASHINGTON — There is a new Internet resource for servicemembers leaving active duty.

Dubbed the DOD Transportal and located at <http://www.dodtransportal.org>, the Web site is designed to be the doorway to Internet transition and job assistance information and services for departing servicemembers and their spouses.

The online service, announced in January, is intended to complement the existing network of transition assistance offices at more than 212 major military installations worldwide.

The Web site has three main features:

* “Transition Assistance” provides a brief overview of the DOD Transition Assistance Program, including

a general discussion of all benefits and services available to servicemembers and their families.

* “At Your Service” provides the locations and phone numbers of all transition assistance offices worldwide and links to other transition-related Web sites.

* “Your Next Career” provides mini-courses on conducting a successful job search campaign and creat-

ing resumes; information on avoiding Internet scams; and links to job search Web sites and corporate recruiting sites.

There is also a suggested reading list of books that can be used as job search resources. (*AFPJ courtesy of Armed Forces Press Service*)



CONTACTS

From previous page

important one: Ask if there's a problem before you cross the line ... not after. When I played football, I can remember being a halfback in a formation flanking out to the sideline, and having to be careful not to set up beyond the line of scrimmage. After being called offside once, I always checked with the referee to see if I had crossed the line. The same approach works with contacts with contractors — check with your JAG, and often.

“Contacts with contractors” becomes more of an issue when contractors and federal employees work next to each other, like Fred and Don. Where the contractor is treated more like a federal employee than a contractor, the scrimmage line has been crossed. Further, the contractor may not join the military in planning sessions when that isn't in the contract. When the contractor acts more like a decision-maker, then it's pushing across the line into “inherently government functions,” and the referee needs to blow the whistle.

The realities of working together have caused a certain relaxation of the old rules, but you still need to check with your legal office when

you get close to the line. Let's take the situation of a contractor and government employee who live near each other in Fairfax, Va., both working in the same office in the Pentagon. Is it permissible for them to car-pool to work?

The Judge Advocate General of the Air Force stated that bona fide car-pool arrangements involving sharing rides between DoD contractors and government employees are not prohibited under the Joint Ethics Regulation. However, this same opinion voiced a concern about appearances when the contractor and government worker, on official travel, share the costs of a taxicab. The opinion stated that this would be permissible as long as each traveler paid his or her proportionate share of the cost directly to the provider of the transportation, but that this practice was recommended as the exception rather than the rule, because of the possibility of the appearance of impropriety.

Let's examine some situations when you clearly are over the line. Don offers a ride to Fred to D.C. for an upcoming conference they both are attending. Fred argues that the contractor is being paid by the government to attend this conference, so that the transportation should be considered as “funded by the govern-

ment,” and he should be able to accept the invitation. However, the answer is “no,” unless the government contract specifically requires the contractor to furnish transportation to government employees. The ride would be considered a gift from a prohibited source that must be declined.

But what if Fred offers to pay Don the fair market value for the transportation to D.C.? It doesn't change things. It's still a gift, and the promise to pay the contractor in the future is not an exception to the gift prohibition.

What if Don invites Fred over for dinner? Is there a long-standing personal relationship? Did the dinner include lobster and steak, so that the gift exceeded \$20? Should Fred decline anyway, since this may create an appearance of impropriety? There is no clear line in this situation; in fact, it's rather gray. Don and Fred are friends who might occasionally invite each other over for dinner, but where do you draw the line?

As you can see, seemingly innocent situations may lead to problems for individuals and their employers. Again, the thing to remember is, when you get close to that line, play it safe: Check with your legal office.

Tinker home to high frequency global communications

By Ami Bui

Oklahoma City Air Logistics Center Public Affairs
Tinker AFB, Okla.

The High Frequency Global Communications System Program Office recently stood up as a new division under the Airborne Accessories Directorate in the Oklahoma City Air Logistics Center here.

The SPO is installing new systems to create a state-of-the-art automated high frequency network to communicate by voice and data with HF-equipped military aircraft. Fourteen worldwide stations will support the effort.

The office ensures ground-based HF radio stations have the most efficient connectivity to communicate with Department of Defense aircraft anywhere in the world.

"Despite the fact many consider HF radio to be 'old hat,' HF and satellites are the only long-haul communications modes available," said Col. Ceasar Sharper, SPO director. "Satellite communications are very expensive and become congested during global crises.

"Today, HF competes favorably with satellites for many kinds of communications due to its very low operating cost and technology improvements during the past several years that make it nearly as easy to use as a telephone," he said.

The HFGC system is used primarily to support four different missions, Colonel Sharper said.

"The primary mission, or global mission, is command and control for mobility air forces such as Air Mobility Command's C-17 (Globemaster IIIs) and (KC-135 Stratotankers)," the colonel said.

The system also supports special aircraft missions for the presidential fleet, the chief of staff and Mystic Star.

"As they're out flying to other countries, operators make sure they have an open line of communications established on our HF network," Colonel Sharper said.

A third mission is System of Telecom Information for American Air Forces. This is a Spanish-speaking communications network that provides administrative and logistics support among all North, South and Central American air forces for the system of cooperation among the American air forces.

The division's fourth mission is to manage the Defense Communications System High Frequency entry, which provides a HF port for global communications for regional commanders.

The office is a communications system acquisition program office, according to Phil Woodring, deputy director.

"This is not something traditionally found at an air logistics center," he said. "Most of our activity is acquiring a new system for the Air Force, not just the modification and sustainment business."

The system's program director and sustainment functions were previously located at McClellan AFB, Calif., while the acquisition segment of the SPO was at Tinker.

"As a result of the base realignment and closure decisions, the two functions merged, and the McClellan faction joined the 25 Tinker people," Woodring said. "Effective this past June, we formally became part of the Oklahoma City Air Logistics Center."

Some equipment the division sustains dates back to the 1950s, "but much of that older equipment has already been retired and few of our stations still operate with it," Woodring said, adding that all of the old equipment will be phased out by the end of fiscal 2002.

"The new string of equipment allows continuation of the same missions the (old ones) had, which provide the communications infrastructure so aircraft can talk to the ground and vice versa," Colonel Sharper said.

"Our equipment also provides significant manpower savings," he said. "This efficiency and effectiveness of the new system means the Air Force can save more than 255 manpower billets to use for other purposes. This equipment has a higher availability rate, which means it rarely breaks."

To further enhance HFGC, the division developed an airborne e-mail capability that allows messages, maps and other communications to be sent to or from aircraft via HF and the worldwide network. Today, communication between ground and aircraft must occur by voice over the radio, which often ties up critical command and control communications circuits.

This new technology insertion will first be operationally introduced in the E-3 Sentry airborne warning and control system fleet by December 2001, said Woodring.

"HF e-mail is a mission enabler allowing the warfighter to communicate air tasking orders, a quick response capability that is not easy for them to do today," said Colonel Sharper. "The information pathway will be encrypted for classified material.

"Bottom line is that our system can support voice conversations and HF e-mail capabilities at the same time," said Colonel Sharper. "The technology gives e-mail a much longer transition range. In the future, our customers will be able to send or receive e-mail with attachments to or from any equipped aircraft in the world." (*AFPN courtesy of Air Force Materiel Command News Service*)

Pentagon comm member's work earns him a promotion

By Tech. Sgt. Mona Ferrell
*Air Force Pentagon
Communications Agency
Public Affairs
Washington*

A member of the Air Force Pentagon Communications Agency has been rewarded for hard work and dedication by being promoted to master sergeant under the Stripes for Exceptional Performers program.



Sergeant Hester

Master Sgt. Thomas S. Hester, AFPCA's NCO in charge of executive telephony services, received the good news Jan. 9, joining an elite group of about 400 other Air Force NCOs promoted under the program annually. STEP allows commanders to immediately promote individuals with exceptional potential when, in their judgment, it is clearly warranted.

Sergeant Hester's outstanding leadership abilities, combined with his job performance and initiative, unmistakably set him apart from the rest, said Col. Joseph E. Laposa, AFPCA commander. "Tom is a very inspirational and goal-driven NCO," he said. "His knowledge in telecommunications is just part of the total package. He goes above and beyond the call of duty in everything he does. Tom's commitment to the Air Force and his community sets the example for others to follow. This is one of the best parts of my job – when I can not only recognize someone for a job well done, but promote them for it. I can't think of anyone more deserving."

Throughout the award period, Sergeant Hester led four people while managing more than 2,000 command and control leased telecommunications circuits and equipment worth

\$10 million in direct support of the Joint Staff and the Secretary of Defense's most vital and secure communications systems.

In addition, because of his superb on-the-job knowledge, Sergeant Hester was handpicked to respond to an expedite STU-III outage at the Chief of Staff of the Air Force's residence. His outstanding troubleshooting skills allowed him to rapidly analyze the outage symptoms, pinpoint the problem and replace the bad telephone set, resulting in less than one hour of downtime.

Using the spirit of giving as a driving force, Sergeant Hester also applied his dynamic leadership skills to initiate the first-ever AFPCA-sponsored Children's Christmas Gift fundraiser. His organizational skills and savvy publicity campaign allowed the agency to collect more than 250 presents and \$400 of donations for the Children's National Medical Center in Washington, D.C.

Surprised by the promotion, Sergeant Hester said, "I was totally blown away and I didn't know quite what to say. I feel very honored and privileged to receive this, because I know there are a lot of deserving NCOs in this agency and to be considered the best of the best is a true honor. Of course, I've met a lot of professionals during my four years here (at the Pentagon), who have served as examples to me. I definitely did not get to this point on my own."

Sergeant Hester, a native of Lakeland, Fla., is definitely deserving according to Master Sgt. Doug Schinn, AFPCA chief of executive telephony services. "Tom seems to know every facet of this job," he said. "He's very thorough — everything he accomplishes is done to 110 percent of his abilities. In addition, his commitment and positive representation of the Air Force puts the 'We Are All Recruiters' program into action on a continual basis. I can't think of anyone more deserving of a STEP promotion."

Help Wanted

Arkansas Air National Guard

The 223rd Combat Communications Squadron, Hot Springs, Ark., has traditional Guard vacancies for individuals who are separating from the active duty Air Force or are qualified for the Palace Chase or Palace Front Programs in the following AFSCs: 2E1X1-Satellite, Wideband & Telemetry Systems; 2E2X1-Communication, Network, Switching & Crypto Systems; 3COX1-Communications/Computer Systems Operations; 3C251-Communications/Computers Systems Control. There's also a position available for a communications officer.

For more information, contact Master Sgt. Kenneth R. Esaw I, at DSN 731-6876 Ext. 226, or call 1-800-631-0509.

New Hampshire Air National Guard

The 157th Air Refueling Wing, Newington, N.H., is hiring personnel in the following AFSCs: 2E1X3-Ground Radio Communications; 2E1X4-Intrusion Detection System; 2E6X3-Telephone Systems; and 3A0X1-Information Management. New Hampshire offers 100 percent college tuition to state schools on a space available basis.

For more information, contact Master Sgt. Norma Long, at DSN 852-3508, or 1-800-257-9368.

Air Force Association honors AFPCA civilian

Story and photo by
Tech. Sgt. Mona Ferrell
Air Force Pentagon
Communications Agency
Public Affairs
Washington

A member of the Air Force Pentagon Communications Agency has been honored with the Air Force Association Outstanding Civilian of the Year Award for 1999.

David V. Bauch, AFPCA electronic equipment maker, installer and repairer supervisor, was lauded Jan. 16 at a Pentagon ceremony for his efforts in the command and control systems arena. Lt. Gen. John L. Woodward Jr., Headquarters Air Force Deputy Chief of Staff for Communications and Information, and Jim Hannam, D.W. Steele Chapter AFA president, took part in the ceremony.

During 1999, Bauch's daily responsibilities included directing the National Military Command Center's elite command and control radio and television maintenance branch. Managing 17 C2 systems for the nation's top military and civilian decision-makers, this branch ensured the President of the United States, the Secretary of Defense, the Chairman of the Joints Chief of Staff and the Joint Staff had superb C2 and audio-visual capability available at all times.

In addition, during Operation Allied Force, Bauch downlinked aerial reconnaissance video feeds from Kosovo and channeled them through NMCC crisis space. He also established fiber connectivity to simultaneously

"Although this is an individual award, it's not something that I won alone. I have a fantastic group of technicians in the TV shop working for me. This award is just as much theirs as it is mine."

David Bauch

throughout the military operation.

Bauch, a native of Rochester, N.Y., was both humbled and honored by the award. "Although this is an individual award, it's not something that I won alone," he said. "I have a fantastic group of technicians in the TV shop working for me. This award is just as much theirs as it is mine."

A former enlisted member, Bauch also credits his strong military foundation and a mentor as being driv-



Lt. Gen. John L. Woodward Jr., Headquarters Air Force Deputy Chief of Staff for Communications and Information, (left) and Jim Hannam, D.W. Steele Chapter Air Force Association president, Washington, D.C., (right) present the 1999 AFA Civilian of the Year Award to David V. Bauch.

record feeds from eight unmanned aerial vehicles, dramatically improving the NMCC's command and control capability, and support to the Joint Staff

ing forces throughout his career. "My military background taught me discipline and adherence to detail – doing things not only expeditiously, but doing them right," he said. "I also think there's a lot to be said about having a mentor. William Love, my predecessor, retired five years ago after 46 years of government service. He was a great mentor with a very distinguished career. I've always tried to emulate him and follow in his footsteps."

This can-do attitude towards teamwork and doing things right is reflected in his leadership and technical abilities, said Capt. Ray Powell, AFPCA C2 systems maintenance chief. "Dave runs an incredibly effective shop. His folks are able to take some of the NMCC's most complex, cutting-edge, and high-profile projects through every stage – from cradle to grave," he said. "They plan, engineer and install their own solutions, saving the government hundreds of thousands of dollars in contracting costs. What's more, he runs what must be the happiest work center I've ever seen – that's not always easy to do."

Dedication to the job, like that continuously exhibited by Bauch, is what this award is all about, Hannam said. "It's a great honor and pleasure to join General Woodward in presenting the AFA Outstanding Civilian of the Year award to Mr. Bauch," he said. "His exemplary leadership abilities and continuous striving for excellence is indicative of what this award is all about."



Awards

Annual Awards

Scott AFB Outstanding Civilian of the Year Category I

Lyn Haar
Air Force Communications Agency

Scott AFB Outstanding Civilian of the Year Category II

Patricia Katzer
Air Force Communications Agency

Company Grade Officer

1st Lt. Gregory A. Davis
786th CS, Ramstein AB, Germany
Capt. John Dunks
509th CS, Whiteman AFB, Mo.

Senior NCO

Master Sgt. Karin M. Ruppelius

786th CS, Ramstein AB, Germany
Master Sgt. James B. Garner
509th CS, Whiteman AFB, Mo.

NCO

Tech. Sgt. Roslyn Lee
86th CS, Ramstein AB, Germany
Staff Sgt. Patricia H. Hope
509th CS, Whiteman AFB, Mo.

Airman

A1C Matthew R. Wells
86th CS, Ramstein AB, Germany
SrA Kristoffer E. Helfert
509th CS, Whiteman AFB, Mo.

Category I Civilian

Ida Gonzalez
786th CS, Ramstein AB, Germany

Category II Civilian

Jose E. Rodriguez
786th CS, Ramstein AB, Germany

Civilian

Steve Profer
509th CS, Whiteman AFB, Mo.

First Sergeant

Master Sgt. Timothy F. Delaney
786th CS, Ramstein AB, Germany

USAFE Lt. Gen. Leo Marquez Awards

Company Grade Manager

1st Lt. Tristan A. Morel L'horset
86th CS, Ramstein AB, Germany

Supervisor Manager

Master Sgt. Ronald E. Rouse

86th CS, Ramstein AB, Germany

Technician Supervisor

Staff Sgt. Richard D. King
86th CS, Ramstein AB, Germany

Maintenance Effectiveness Award Large Unit

86th CS, Ramstein AB, Germany

Quarterly Awards

CGO

1st Lt. Warren E. Vines
*Headquarters Air Force Deputy
Chief of Staff for Communications
and Information
Washington*

Civilian

Michael C. Mehrman
*Headquarters Air Force Deputy
Chief of Staff for Communications
and Information
Washington*

Senior NCO

Master Sgt. Allen E. Illg
*Headquarters Air Force Deputy
Chief of Staff for Communications
and Information
Washington*

Individual Mobilization Augmentee

Lt. Col. Salvador E. Battle
*Headquarters Air Force Deputy
Chief of Staff for Communications
and Information
Washington*

See **VALOR** Page 30

Valor & Recognition

If you've received an award, promotion, or some other newsworthy event, tell the rest of the Communications and Information community. Send an e-mail to intercom@scott.af.mil or mail it to AFCA/XPPA (*intercom*), 203 W. Losey St., Room 1200, Scott AFB IL 62225-5222

ABS	Air Base Squadron
ACOMS	Air Communications Squadron
AFCA	Air Force Communications Agency
AFFMA	Air Force Frequency Management Agency
AFCQMI	Air Force Center for Quality and Management Innovation
AFPCA	AF Pentagon Communications Agency
AFSOC	AF Special Operations Command
AFTAC	AF Technical Applications Center

AFWA	Air Force Weather Agency
ASOS	Air Support Operations Squadron
CCS	Combat Communications Sq
CG/Comm Gp	Communications Group
CLSS	Computer Logistics Support Sq
CS	Communications Squadron
CSG	Computer Systems Group
CSO	Computer Support Office
CPSS or CSS	Computer Systems Squadron
DISA	Defense Information Systems Agency
EIG	Engineering Installation Group
EIS	Electronics/Engineering Installation Squadron
JCSE	Joint Communications Support Element
MSG	Materiel Systems Group
RSG	Regional Support Group
SSG	Standard Systems Group

VALOR
From Page 29

Medals



Defense Meritorious Service Medal

Senior Master Sgt. Steven Hannah Sr.
509th CS, Whiteman AFB, Mo.



Meritorious Service Medal

Master Sgt. Lucy M. Johnson
Master Sgt. Franks S. Lucero
Master Sgt. Angela K. Williamson (1OLC)
509th CS, Whiteman AFB, Mo.



Joint Service Commendation Medal

Staff Sgt. Dwayne Forde
509th CS, Whiteman AFB, Mo.



Air Force Commendation Medal

Tech. Sgt. Ronerick M. Woolen (2OLC)
Tech. Sgt. Stephen J. Boatman (3OLC)

Staff Sgt. Gene E. Kapuchuck (1OLC)
Staff Sgt. Kristopher F. Krug (1OLC)
Staff Sgt. Michael C. Koonce
Staff Sgt. Michael B. Alexander (1OLC)
509th CS, Whiteman AFB, Mo.



Joint Service Achievement Medal

Tech. Sgt. Gerald L. Aguilar
Staff Sgt. Michael G. Guyton, Jr.
Senior Airman James Witte
509th CS, Whiteman AFB, Mo.



Air Force Achievement Medal

2nd Lt. Justin M. Loosvelt
Master Sgt. Angela K. Williamson (3OLC)
Tech. Sgt. Daryle G. Christensen (4OLC)
Staff Sgt. Reginald L. Chandler
Senior Airman Nicholas C. Horton
Airman 1st Class Donald M. Popham
509th CS, Whiteman AFB, Mo.

If you would like to have your unit or someone in your unit recognized in the *Valor and Recognition* section, please e-mail that information to intercom@scott.af.mil.

Former AFCC member dies

A former Air Force Communications Command Deputy Chief of Staff for Logistics, Col. Ole I. Dahle-Melsaether, died Jan. 25 at the Scott AFB Medical Center, Scott AFB, Ill.

The colonel retired in 1989 after 37 years in the Air Force, and resided most recently in O'Fallon, Ill. His last Air Force assignment was as the Airlift Communications Division Director of Operations at Scott.

He was born Sept. 16, 1932, in Mossbank, Saskatchewan, Canada. After graduating from Decorah High School, Decorah, Iowa, in 1950, he enlisted in the Air Force in January 1952 as an air traffic controller. In 1959, he was selected for Officers' Candidate School and upon completion was commissioned as a second lieutenant.

After graduation from Officers' Ground Electronics School, Keesler AFB, Miss., in 1960, he was assigned to Eufuala Air Force Station, Ala.

The colonel also served in northern Europe, Republic of China, Korea, New York, Missouri, Minnesota, Montana and Illinois.

Surviving are his wife, Maureen, two sons and a daughter: Maj. Bryan Dahle-Melsaether, of Las Cruces, N.M., and Capt. Mark Dahle-Melsaether of Colorado Springs, Colo.; and Dawn Dahle-Melsaether of St. Louis, Mo. He is also survived by two brothers, Oscar Dahle-Melsaether, of Manly, Iowa, and Philip Dahle-Melsaether, of New Brighton, Minn.; and his sister, Anna Christiansen, of Arlington Heights, Ill.; as well as two grandchildren, Karleigh and Jacob.

intercom

special focus issues, deadlines for submissions

May - Information Management (deadline - March 28)

June - People First (deadline - April 27)

July - Better Ways of Doing Business (deadline - May 30)

August - Information Technology Initiatives (deadline - June 28)

September - New Comm & Info Technologies (deadline - July 31)

October - Almanac edition (deadline - Aug. 30)

November - Global Information Grid (deadline - Sept. 28)

(watch for updates/changes to themes)

Sergeant gives brother gift of life

By Airman 1st Class Chris Uhles
49th Fighter Wing Public Affairs
Holloman AFB, N.M.

Philosopher, poet and novelist George Santayana once said, "The family is one of nature's masterpieces." To protect those masterpieces, some people will give up just about anything.

Staff Sgt. Harry Fisher is one of those people.

Sergeant Fisher, a videographer with the 49th Communications Squadron Visual Information Center, is recovering from donating a kidney to his older brother, who suffers from membranoproliferative glomerulonephritis, a disease that caused his kidneys to shut down.

In what many are calling a heroic effort, and what he tries to downplay, Sergeant Fisher underwent a kidney removal procedure called laparoscopic nephrectomy.

The new procedure, which had been performed only a dozen times in New Mexico, leaves the donor in much better shape, said Barbara Morgan, pre-transplant coordinator for Renal Medical Associates, in Albuquerque, N.M. The previous method meant the donor would be hospitalized at least nine days, Morgan said, and would be out of work for six to 10 weeks. With this new procedure, donors can leave the hospital after three or four days and return to work in less than six weeks.

The effects of losing this major organ are minimal, she said. "A person can live a very healthy and normal life with only one kidney. In fact, there are many people who are even born with only one kidney."

"I don't feel any different, just sore," Sergeant Fisher said. "All I had to do was lie there and let them take the kidney. The real heroes are the people that surround me: my wife, who had to take care of everything while I was recovering, and my coworkers, who had to pick up my slack in my one-deep position. Those are the people who did something, not me."

Sergeant Fisher's supervisor disagrees.

"It was his sacrifice that was great," said Tech. Sgt. Alex Ray, Visual Information superintendent. "Whatever we can do to support him in this is small potatoes compared to what he did."

Sergeant Fisher's brother's kidney began to fail last year and a donor was needed. The sergeant volunteered one of his kidneys and he turned out to be a perfect match. In fact, the doctors were surprised at how close a match Sergeant Fisher was. Morgan explained the uniqueness.

"Each candidate for donation is probed and prodded. No stone is left unturned. We have to make sure there are no underlying diseases that could put the kidney at risk later on.

"Each candidate has to be very healthy," said Mor-



Photo by Staff Sgt. Sam Park

Staff Sgt. Harry Fisher explains his job to Gen. John Jumper, Air Combat Command commander, during the general's visit to Holloman Air Force Base, N.M., in November.

gan. "They get several physical exams, lab tests and a CAT scan to ensure the kidney will function properly. The closeness in type of Harry and his brother is usually only found in identical twins."

Did that help in Sergeant Fisher's decision process?

"There was no question," said Sergeant Fisher. "I didn't even give it a second thought. It's my brother. Giving him the kidney gave him a second chance at doing what he wants in life. He's got a wife and two kids. Now he's got a whole new life. I had no hesitation."

The sergeant also explained being in the Air Force helped him make the decision.

"All those times I've had to deploy with the Air Force were not necessarily something I wanted to do, but I knew I had to do it and move on," said Sergeant Fisher. "That really helped me in my decision."

The NCO said he was "a little nervous about the surgery," but knew his brother would do the same for him.

"The weirdest thing about the whole ordeal was walking into the hospital and surgery room completely healthy, and leaving hurt," said Sergeant Fisher. "But I'd do it again in a heartbeat." (Courtesy of Air Combat Command News Service)

