

intercom

April 2002

**Air Combat Command
Comm and Info**

**Enabling Combat
Air Forces**



intercom

Volume 43, No. 4

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

Contributing Editors
Capt. Jerome Cobb
and Capt. Stamatis Smeltz
Air Combat Command Comm and Info

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/PA, *intercom*, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222. Fax is DSN 779-6129 or (618) 229-6129. Editorial staff may be contacted at DSN 779-5690, or (618) 229-5690.

Check out
our Web site at:

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



ACC comm and info

6 JEFX builds air operations center of the future

8 55th CS airman on point for Enduring Freedom



12

10 609th ACOMS builds comm capability for OEF

12 Communicators overcome training obstacles

16 5th CCG leads change in deployable comm



8

18 ACC postal supports Enduring Freedom

20 ACC meets challenges of C2 'sysads'



18

IA Campaign 2002



22 Remanence security essential to protect electronic information

25 What to do if you find classified info in your e-mail

26 Properly disposing of electronic data is vital

in other news

30 Retired comm leader dies at age 66

32 Air Force IT leaders receive recognition

34 Senior officers reassigned



30

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

About the cover

This month's cover focuses on Air Combat Command communications and information.



Cover by Tech. Sgt. Mike Leonard

ACC comm and info warriors continue transformation journey

By **Brig. Gen. Michael W. Peterson**
*Communications and Information Systems
Director
Air Combat Command
Langley AFB, Va.*



“Those hours and minutes we give back to each airman with information technology tools and updated processes translate directly into increased combat power.”

**Brig. Gen.
Michael W. Peterson**

The buzzword is “transformation,” but I don’t believe it’s just a passing fad for members of the Air Combat Command communications and information team. It’s something we’ve been working, and working hard, for the past decade. It’s also an attitude that will carry us into the future. Transformation for the Air Force means integrating all of its diverse capabilities into powerful, desired effects, like linking the attributes of space, air and information systems into seamless warfighting entities. You notice I said, “linking.” I did that on purpose, because much of the transformation taking place in our Air Force relies on communications and information systems, built around sound operational concepts and innovative processes. On the expeditionary combat support front, it’s also the opportunities provided by modern information technology that are paving the way for new processes, and delivering resource savings which we can plow back into our operational force – paying the bills through re-engineering and transformation, and not by doing more with less.

Communications is being considered in a different light. In our ongoing war on terrorism, new Intelligence, Surveillance and Reconnaissance platforms have revolutionized information flow to the joint forces air component commander and senior commanders across the board. In years past, commanders and intelligence leaders would have been content to follow the status of platforms, sensors, analysis teams, and the hardware at each node in the TPED (tasking, planning, exploitation and dissemination) process. Not any more. Today, senior commanders are also briefed and remain keenly interested in the information enterprise which links each of those separate pieces together. They also understand the next fight we enter will require even more robust and better managed networks to meet the needs of our commanders. It’s our job to

plan and build those networks, including elements which deliver key information right down to the individual unit, flight, targeteer and crew member.

Actually, transformation has been part of our communications and information vernacular for the past decade. Initiatives like ACCWay (a computer store that provides Web-based access to multiple vendors offering ACC compliant desktop and laptop computers), Virtual Management Level Review, Automated Processing (in- and out-processing on the Web), and many more projects were designed for one thing: to rely on technology to drive down the manpower bill associated with so many of our day-to-day tasks. Those hours and minutes we give back to each airman with information technology tools and updated processes translate directly into increased combat power.

Best of all, more is coming. None of us wants to drop a key project or critical task to run to the finance office to work a minor pay issue. Most of us simply put off the visit until the last minute. What we need is an online, secure capability to deal with our pay and personnel matters at a time convenient to us as individuals – the good news is that’s exactly what’s coming ... and coming soon. So are many more initiatives to drive down the manpower bill associated with combat support functions. You will hear of them and see them

See **TRANSFORM** Page 4

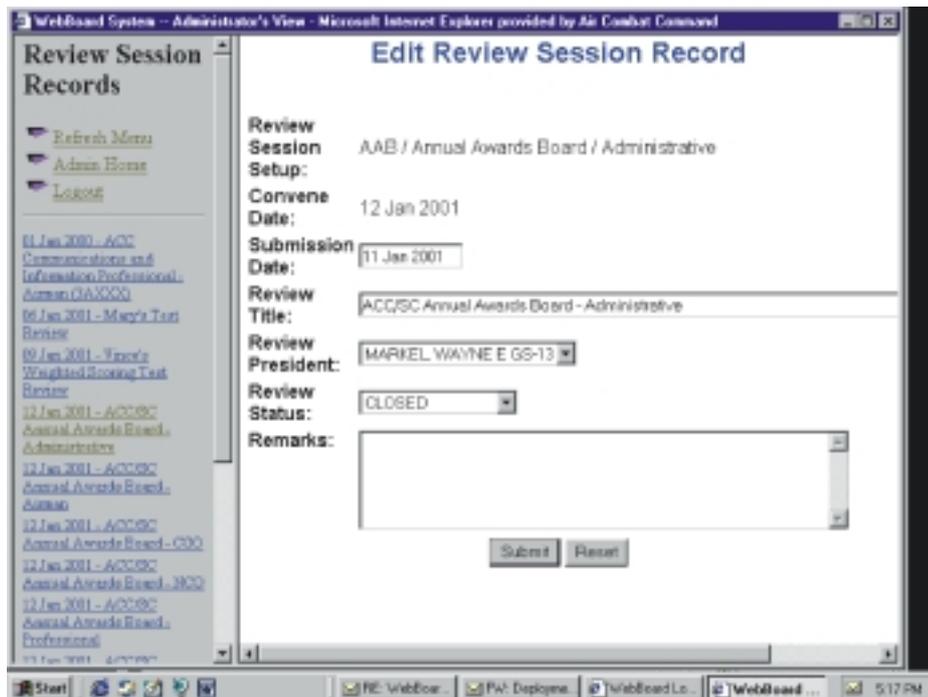
TRANSFORM

From Page 3

implemented in the very near future. Those initiatives must come from the experts closest to the problem – you! Fight for the good ideas you know will work and which will make our precious resources deliver the effects we desire at reduced costs, both in manpower and in dollars spent.

In our own community, significant shortfalls exist in specialties and organizations we need the most. There never seem to be enough experienced work group managers, systems administrators, information managers, or equipment maintenance technicians to do all the work. The Air Force recognizes those shortfalls, but doesn't have the resources to easily bail us out. I think we're smart enough to do much of that work on our own. We can re-engineer or "transform" internally to work smarter, rely on improved tools, and push critical resources to the areas feeling the greatest pain.

We've already done much, like running the U.S. Central Command area of operations Network

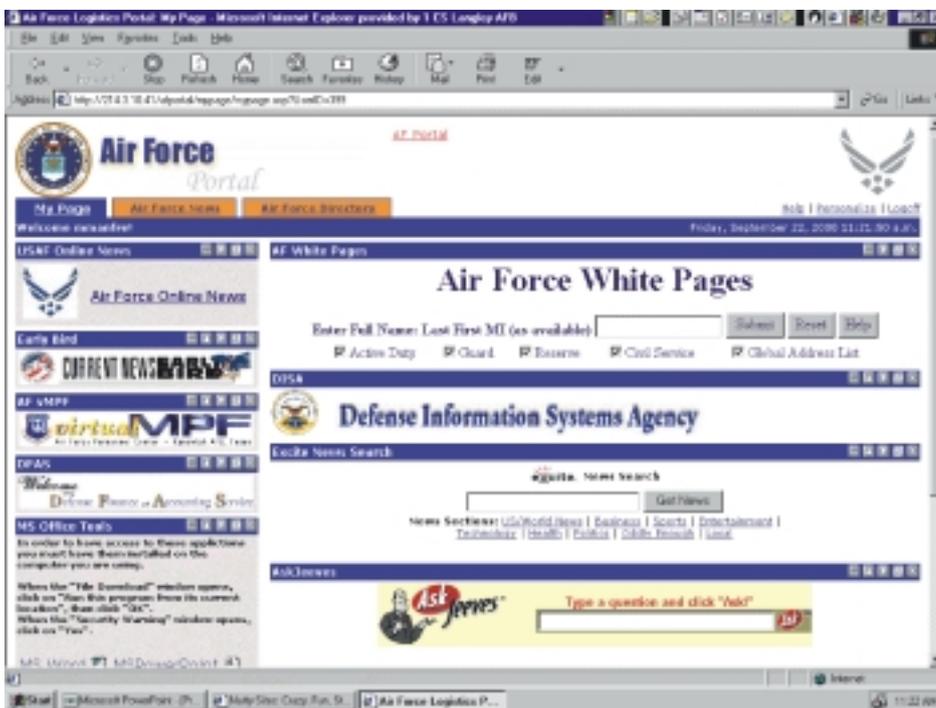


Virtual Level Management Review

Operations and Security Center – Deployable, using a remote-based concept of operations, which cuts down dramatically on the expeditionary manpower bill. We can, and are, doing more. New tools are coming to our network control centers and the ACC NOSC which will allow us to roll some responsibilities up to the ACC NOSC. Doing the work centrally cuts down on NCC training require-

ments and allows the work to be done with less manpower – the NCCs are already putting those manhour savings to good use, catching up on the backlog of work which was going undone.

Each of us has experienced the transformation undergone by our information management community, with centralized publishing, outsourced printing services, and now on the horizon, electronic records management. Now isn't the time to rest on these important improvements. We must continue to move forward with additional ideas, processes and attitudes. For expeditionary combat support, information management will evolve into



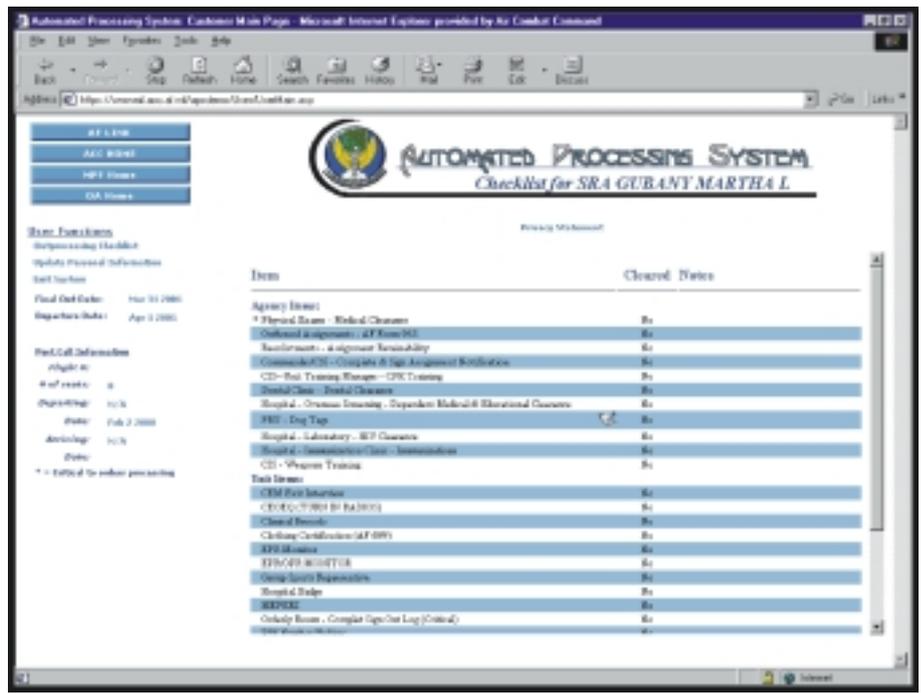
Air Force Portal

the Air Force Portal, with full exchange and flow of information across every functional application which supports us. Even more exciting is the recognition that information management has a critical role to play on the floor of our combined air and space operations centers. Experience from earlier exercises and the implementation of a new command center at 1st Air Force in support of Operation Noble Eagle makes it perfectly clear that information management is the pathway to future CAOC improvements.

Another initiative to save resources – like tech refresh dollars, manpower and implementation costs – is information technology consolidation. Industry has proven repeatedly that consolidating applications servers, physically or virtually, results in an environment where fewer technicians can care for the systems. It also results in an environment where multiple applications can be hosted on fewer machines – fewer machines means less tech refresh dollars when it’s time to replace them. The resulting savings in manpower and dollars can be plowed right back into our “business” of delivering air and space power. In ACC, the situation is perhaps more acute than most would imagine. Across the command, 1,300 personnel who are not trained systems administrators actually provide care for most “functional” servers, like supply, civil engineering and finance. IT consolidation should put a significant number of those people “back on the flight line.”

ACC’s IT consolidation effort is well under way, with core services consolidation nearly complete, and a plan to build central storage and processors facilities in our NCCs. Core services include e-mail, Web browsers, and file-and-print servers. As we grow our ability to centrally host and administer core services, we’ll begin to tackle functional server farms which sprang up on our bases over the past decade. Every manpower authorization we save, or dollar we don’t have to spend on “old processes,” is a resource we can return to the fight – it’s our contribution to the transformation journey.

Most importantly, ideas, initiatives and better ways to get the job done come from everywhere in



Automated Processing System

this command. Years ago, when I was a squadron commander, a young flight commander came to me exasperated because she couldn’t figure out a duty schedule for her personnel assigned to several 24-hour work centers. I suggested she assign the task to two volunteers who actually worked inside the affected facilities. The two airmen who volunteered hit a home run with their effort. They were the only ones who understood the problem: Everyone was trying to pursue off-duty education, but the schedule built by the flight commander just didn’t fit the bill. The schedule the airmen developed was fair, it rotated, and everyone loved it. Fairness was based on everyone working the same schedule, and the schedule rotated every 10 weeks – amazingly, so did the local school semester schedule.

Don’t be content to only make minor changes, or to save the “good ideas” for in-garrison responsibilities. Be bold in what you suggest, and focus first on what works best in an expeditionary environment. You’ll make a difference as an individual, and have greater impact as a member of a team focused on taking charge of “our Air Force” and the way it executes its most critical missions.

It’s up to all of us to continue the transformation journey. It’s our heritage in the communications and information community, and we’re prepared for the task. Keep pressing and we’ll certainly make our Air Force a more effective and capable force.

JEFX builds air operations center of the future

By **Capt. Paul Ettinger**
Chief, JEFX Communications
Air Combat Command
Langley AFB, Va.

The voice on the loudspeaker booms, “BOX IS HOT,” and the air is filled with the crackle of fighter and airborne warning and control system chatter. On three theater-size screens are the tracks of countless aircraft flying missions in the area of responsibility. Tension is thick in the battle cab, as the joint forces air component commander and his staff focus intently on Predator video monitors. They’re going after several priority targets tonight, with one in the crosshairs now. Putting bombs on target is what the Air Force is about, and you’re right in the middle of where it all comes together: the combined air operations center. Functioning as the nerve center of the air campaign for Operations Southern Watch and Enduring Freedom, the CAOC plans, monitors and directs joint search and rescue, theater missile defense, time critical targeting, battlefield coordination, special operations support, sortie execution and countless other mission critical operations.

With hundreds of computers, dozens of servers, racks of video equipment and display screens surrounding you, it might seem like the set of a futuristic movie -- but this is as real as it gets. It’s no small task to ensure AOC systems work together and provide reins of command and control to the JFACC. Making these systems hum requires hundreds of people, working in satellite communications, imagery analysis, network design, computer programming, radio systems, systems administration and many other fields. After the bugs are worked out, the Air Force baselines configuration, and Electronic Systems Center, Hanscom AFB, Mass., manages the pieces and parts as a unified system called USQ-163 – currently block 10 – more commonly known as the air operations center.

Like any weapons system, the AOC is constantly evolving to support mission changes and enable commanders to execute warfighting efforts with confidence. Introducing changes to AOCs in



Photo by Tech. Sgt. Cedric H. Rudisill

A B1-B Lancer carefully moves toward the refueling boom of a KC-10A Extender during a mission in support of Operation Enduring Freedom.

the field is done through the Air Force’s Joint Expeditionary Forces Experimentation efforts. Every two years, the Air Force builds an experimental AOC and conducts exercises to assess system performance, and operational tactics, techniques and procedures. Some of the evaluated systems, such as Theater Battle Management Core Systems, are evolutions of current hardware and software. Others, called initiatives, are intended to be revolutionary “next generation” capabilities seeking to leapfrog current practices. An example is reducing the time-critical targeting chain to less than 10 minutes – from target identification to assessment, vectoring or re-vectoring an aircraft with the proper munitions load, target acquisition and putting bombs on target. Current capabilities take significantly longer, and 10 minutes would be a huge advantage on a battlefield where the situation is constantly changing and the enemy is al-

ways on the move. Leading edge systems and technologies tested during JEFX '02 are seeking to prove their worth and become part of the next AOC block upgrade. HQ ACC/SC's C3 warfighter support division and JEFX communications branch provide communications infrastructure support for the biennial experiments, and lead development efforts for a number of technology initiatives rolled into each exercise.

This year's JEFX experiment will be executed in concert with the joint exercise Millennium Challenge '02, making it our biggest effort to date. The HQ ACC/SC JEFX communications team is working with the 3rd Combat Communications Group and 612th Air Communications Squadron to build an AOC at Nellis AFB, Nev. It will be linked to over 14 sites, including Hurlburt Field, Fla.; Beale AFB, Calif.; Langley AFB, Va.; the USS Coronado; and several U.S. Army, Navy and Marine sites. Most communications links supporting JEFX/MC '02 will work through satellites, with T-1 and T-3 links to selected locations. From a communications perspective, our joint ACC JEFX/Hanscom AFB communications engineering team is taking on challenging tasks that will make a huge difference in how people do their jobs in an AOC.

Working from desktop level to SATCOM links providing bandwidth to the AOC, we're fielding

technology not previously used in an AOC environment. System integration is key to our success, and an example of communications options under consideration is merging AOC voice and data networks using technologies like voice-over Internet protocol, with collaborative tools like InfoWorkSpace. Linking these systems into radio-based command and control nets and enterprise-wide voice networks will allow users to communicate through a single headset wired into a multi-purpose PC. The headset will allow users to communicate with anyone virtually anywhere in the world. JTF/J3 operators could leverage this capability in an audio chat session, viewing imagery or video and discussing what they see with analysts and targeteers, while talking to aircraft over a radio channel, and still listening to the intelligence and targeting discussion. This unprecedented capability would allow passing near-real-time direction to our pilots through a single instrument, eliminating need for a PC, a STE or KY-68 secure phone, or a radio set on the desktop. Preliminary testing has been favorable, and we anticipate making this a part of future AOC architecture. Some other exciting technologies the ACC JEFX communications team may field in the '02 scenario are satellite-based time division multiple-access connectivity, mobile airborne networking, and selective Internet protocol multicasting of intelligence, surveillance and reconnaissance video streams from Predator and Global Hawk platforms to desktop PCs in the AOC.

While we're always looking at introducing new technology to the field, we're also refining use of technologies such as virtual private networking, network management, and overall information management processes supporting AOC operations. Bringing together technology experts and system operators from throughout the Air Force in JEFX experimentation offers a unique opportunity for developing and testing the way we'll fight in the future. Everything we do in the HQ ACC JEFX communications branch is focused on C2 integration and leveraging technology, to get airlift where we need it, when we need it, and to put bombs on target faster and with greater accuracy.



Photo by Staff Sgt. Shane Cuomo

Members of the 405th Air Expeditionary Wing fill sand bags during Operation Enduring Freedom.



Photo by Staff Sgt. P.J. Farlin

OPERATION ENDURING FREEDOM -- Air Base, Spain. Moron AB serves as a stopover point to provide fuel, maintenance and crew-rest for troops supporting OEF.
Airmen from Mountain Home AFB, Idaho, perform last minute checks on an F-15E Strike Eagle prior to takeoff from Moron

55th CS airman on point for Enduring Freedom

By Senior Airman Heather E. Thatcher
*Network Control Center
 55th Communications Squadron
 Offutt AFB, Neb.*

On Sept. 24, a large contingent deployed from Offutt AFB to the desert for Operation Enduring Freedom. Specialties included pilot, in-flight and ground maintenance, intelligence, weather and two communications people: Staff Sgt. Patrick J. Audinet and me. Our task was to provide radio and satellite communications for the 38th Reconnaissance Squadron – primarily aircraft and operations.

We spent our first day in a hangar waiting for a building to be cleared out for our use as an operations center, and our first night pitching our tents in the desert. When the building was available, Sergeant Audinet and I began setting up our radio equipment. After crawling around on the roof assembling antennas, we came inside to discover we had no working phone lines, no DSN capability, no network backbone, no secure Internet protocol router network, and most importantly, no American standard power source to plug equip-

ment into. Since we were the only communications people available, not to mention the only people carrying tools, we were asked to provide any or all of these services until the civil engineer and the mobile communications unit arrived.

Although we couldn't do much about establishing connections to the outside world, we made some progress with the help of communications personnel from airborne warning and control system, and the British Royal Air Force. We used our ingenuity to provide power to the entire building, install a local phone line, and even drop cable to connect computers and create a work group, so users could share resources such as printers and files. We felt a sense of accomplishment in going the extra mile to help get the entire operation off the ground. The chaos of the first few days subsided with the arrival of security forces, civil engineer, communications and other services group people.

Sergeant Audinet and I continued monitoring our radio equipment, while serving as work group manager for Offutt personnel. Although it was a relief to have order restored, I actually missed the

See **55TH CS** next page

April 2002

IT impacts traditional information management

By Chief Master Sgt. Doris H. Hawkes

3A Functional Manager

Air Combat Command

Langley AFB, Va.

Not so long ago, the information manager's toolkit consisted of typewriters, stand-alone word processors, manual mail systems, and paper filing, storage, and retrieval systems to support information management processes and keep office publications, forms, and records current and available. At the dawn of the 21st century, information managers are fueling technology, knowledge and experience to master sweeping changes ahead in their career field.

In Air Combat Command, more than 2,400 information managers are working hard to balance strengths of our IM past with today's tools. They're keeping up with changing technology to create better methods of managing information. Today, information managers have a new weapon, computers – including more than 87,282 in the command – to manage to make their jobs easier and more efficient. They're linking systems and programs into integrated warfighting infrastructures, providing command and control, communications, computer, intelligence, surveillance and reconnaissance capabilities worldwide.

Since October 1996, information managers have been responsible for supporting every user in their organization. This translates to the first 400 feet of network services. Implementing the Air Force Portal, electronic records management, electronic workflow, and storage area networks will significantly change how we manage and control information. The Air Force Portal will provide the front-end link to common user combat support systems to allow us a single interface with today's functional systems. The electronic records management system will give all computer users pow-

erful tools to create, control, collect and disseminate information – covering a substantial portion of the information life cycle. Electronic records management will support combat and combat support systems data to meet our legal and regulatory requirements. Storage capacity needed in the near future will be an order of magnitude greater than what is discussed today, but will eliminate need for warehouse space to store paper, magnetic and photographic media. We'll need to consider how to store exabytes, or millions of terabytes, of data. The system must be able to manage data in a way that it can only be altered by an authorized user, which is a key legal requirement for records management. Another key feature will be assigning every record a disposition that specifies how long it must be maintained, and when it will be ready for destruction or permanent storage.

ACC needs information managers with knowledge of records, administrative communications, publications and forms. This knowledge is fundamental and essential to managing information, whether paper- or electron-based, throughout its life cycle. As ACC continues to provide strategic direction, policy and resources to support four numbered air forces, 17 major bases, and 15 other major units, we applaud our commanders, supervisors and information managers for making great strides towards meeting these requirements.

We must be more effective and efficient in our use of available resources, as we face growing dependence on information technology and greater challenges in managing information resources on more than 800 ACC combat and combat support systems. Effective use of information managers remains the key to managing information, from creation to destruction. The only thing that's changed is the media we use to handle this critical resource.

55TH CS

From previous page

satisfaction derived from being needed and performing well under pressure.

The members of that first group to arrive felt a special bond in being there from the start, and

watching our little corner of the desert grow from some cots in a hangar, to a fully functioning installation. With all my previous experience having been working with the latest equipment in a modern networking shop, I didn't often really feel I was in the "military" – except for the uniform and

the 5 a.m. recalls. OEF gave me a first-hand taste of what we all do for the mission. I'm grateful for having the opportunity to contribute to this endeavor that's currently so prominent in the hearts and minds of all Americans.

609th ACOMS builds comm capability for OEF

By Capt. Brandon Robinson
C2 Systems Flight Commander
609th Air Communications
Squadron
Shaw AFB, S.C.

Since the first bombs of Operation Enduring Freedom dropped on Afghanistan Oct. 7, the media has provided countless stories describing the tools that have made our success possible. Bases appeared out of nowhere in the middle of Pakistan, Uzbekistan, even Afghanistan, and unmanned aerial vehicles such as Predator and Global Hawk made daily headlines. Along with rapid deployment of troops and cutting-edge technology, communications requirements were equally unprecedented, but largely taken for granted. The heroic efforts of the 609th Air Communications Squadron helped assure success.

In 1999, 609th ACOMS, also known as U.S. Central Command Air Forces A6, began planning Operation Desert Shift, the move of the combined air operations center, joint intelligence center, and Joint Task Force – Southwest Asia Headquarters, from Eskan Village to Prince Sultan AB, Saudi Arabia. While the transition was primarily motivated by force protection, the 609th viewed it as an opportunity to build a modern CAOC facility that could meet increasing C4 demands of air campaigns.

For Desert Shift, ACOMS spearheaded construction of the Air Force's first operational AN/USQ-163 Falconer aerospace operations center weapons system at Prince Sultan. This system became the new CAOC, designed to greatly increase operational capability of its Eskan-based predecessor. The 609th took the lead in this massive project, working with engineers and logistics support personnel from Electronic Systems Center; Air Force Communications Agency; Air Force Command and Control, Intelligence, Surveillance and Reconnaissance Center, and other organizations. After building, equipping, installing and testing the \$50 million leading-edge weapons system in the new 72,000-square-foot complex, the 609th ACOMS turned over to JTF-SWA the world's



Photo by Staff Sgt. Shane Cuomo

A weapons loader from the 28th Air Expeditionary Wing gives a signal that the 2,000-pound bomb he prepped is ready for loading on a B-1 bomber for Operation Enduring Freedom.

premier C2 facility.

The 609th ACOMS deployed more than 100 personnel from diverse communications and information career fields for an average of 100 days, working 12-14 hour shifts around the clock to install, configure and operate more than 50 C2 systems, 300 work stations, seven radio networks, and 350 commercial and tactical telephones used by warfighters to perform missions directed by the commander, USCENTAF. These capabilities were built on an infrastructure of 5,000 miles of fiber, coaxial, and category five cable, installed by 21 Air National Guard engineering and installation teams.

The CAOC became operational in August, providing a fully-integrated, interoperable common air picture and airspace management system. It also fused communications and intelligence, battle management, theater missile defense notification, weather picture, and common-user C2/C4 services, all riding an operational coalition network and integrated U.S., host nation and commercial backbone. The system allows COMUSCENTAF to exploit, to the maximum, current innovative technologies that enhance C2 coalition air forces' ability to execute theater missions.

Though the 609th designed the CAOC complex to meet requirements of "tomorrow's fight," they didn't realize that fight would literally come "to-

morrow.” No one envisioned that within days of the facility becoming operational, terrorists would attack our nation Sept. 11. As a result, the Falconer weapon system became the main center of gravity for prosecuting OEF, in addition to Operation Southern Watch.

Even with the world’s premier C2 facility in operation, much work was yet to be done to robust the theater for conducting OEF. Immediately after the terrorist strikes, the 609th ACOMS crisis action team was activated to coordinate taskings the unit was about to undertake. A “prepare-to-deploy” order was given to start what eventually became OEF. A KC-10 flew into Shaw AFB, S.C., and carried Lt. Gen. Charles Wald, 9th Air Force commander, and his advance echelon staff to the CAOC.

After the general and his initial staff – including 11 609th personnel – were in place, coordinating the bed-down of deploying forces was begun. In a mere three weeks, the Air Force began movement of its initial forces, in large part to established locations. However, the bare-base scenarios magnified the level of difficulty. The ACOMS met the challenge by setting requirements for tactical infrastructure, generating satellite access requests, planning circuit routes and data paths for these austere locations, and building a comprehensive initial time-phased force deployment document to call out the necessary resources and unit type codes required for the operation. Within a month, six new bare-base locations sprang up across the theater, as tactical communications units quickly established required communications and computer network support.

In order to meet demands placed on the new CAOC, the 609th quickly deployed 20 communicators to augment the CAOC and JTF-SWA/J6 staff. The mission was to support the growing area of responsibility from within the CAOC by standing up a plans cell within the C6 staff, adding theater battle management core systems administrators to the CAOC operations floor, and augmenting operators within the Joint Communications Control Center.

Back in CONUS, the squadron’s theater management flight was working overtime to provide systems and long-haul bandwidth necessary to support almost-daily arrival of bandwidth-intensive intelligence, surveillance and reconnaissance systems, such as Predator, Global Hawk, and Joint STARS, along with communications requirements for new bases in-theater. Through aggressive

implementation of global broadcast system, commercial satellite initiatives, and more effective bandwidth management, a tenfold increase in theater bandwidth was achieved.

To manage this increase in data network infrastructure, the 609th’s Network Operations and Security Center – Deployable robusted its operations. In 1999, the squadron established the first NOSC-D, providing 24-hour network monitoring and troubleshooting of a deployed network. By leveraging modern commercial off-the-shelf enterprise management tools, the NOSC-D was able to deploy in-place at Shaw AFB, thus providing virtual in-theater support from the continental U.S. Since no additional manpower was provided for this mission, the 35 military, civilian and contract personnel in the NOSC-D, supporting six bases in Southwest Asia, were matrixed from other parts of the squadron. With the onset of OEF, the NOSC-D had to provide network management of seven additional sites. Because of additional deployed requirements for the new sites supporting OEF, ACC was unable to send augmentees to the NOSC-D. The Air National Guard met the challenge by providing 27 personnel from several units, making the 609th ACOMS a true “Total Force” unit. The NOSC-D could then effectively manage the 64 firewalls, 13 TBMCS virtual private network enclaves, 28 routers and 28 domain name servers in the AOR.

When sites supporting OEF were in early stages of activation, theater deployable communications packages brought by the deployed communications units often contained equipment that was outdated or insufficient to support demanding operations. The NOSC-D filled shortfalls by deploying three teams to augment the TDC packages, installing 72,000 pounds of equipment worth \$12 million at six sites. This amazing effort was accomplished in less than a month, thanks to assistance of ANG augmentees and AFCA’s Scope Network team.

Building the network was only part of the job – it also had to be protected. The NOSC-D coordinated with 9th Information Warfare Flight, Joint Communications Control Center, Central Command J6, and Air Force Computer Emergency Response Team to secure the network from hackers at theater entry points. The solution involved sending teams to field Cisco secure intrusion detection systems behind “tier 0” connections and fielding

Communicators overcome training obstacles

By Capt. Robert A. Harrington
Team Leader, Training Strike Team
3rd Combat Communications Group
Tinker AFB, Okla.

Training has always been the lifeblood of the 3rd Combat Communications Group, also known as the 3rd “Herd,” at Tinker AFB. Constant preparation is required to be effective “Anytime ... Anywhere,” as stated in the unit motto. As recently as six months ago, high ops tempo, high personnel turnover and manning shortfalls threatened the group’s ability to train.

Col. Gregory L. Brundidge, 3rd CCG commander, acknowledged this fact by saying, “We aren’t going to get more resources. Doing more with less won’t cut it,” he said. “We need to find smarter ways to use what we already have.”

To combat threats to combat communications training, Colonel Brundidge appointed a team of the 18 best training experts from the group’s five squadrons. They represented all levels, including trainees, trainers, work center supervisors, superintendents, flight commanders and group training staff. The team called itself the “3rd Herd Training Strike Team.”

The TST developed 14 initiatives addressing training processes and environment. The most significant of these initiatives included establishing functional cadres and improving schedule predictability.

These functional cadres were cross-squadron leadership teams that focused resources on similar group functions. Simply put, they promoted sharing of skilled trainers and training equipment between squadrons. This optimized group resources and reduced interruptions in training due to deployments and personnel turnover.

The Herd’s four functional cadres include base-level systems, network systems, airfield systems and combat support. A mission squadron commander leads each cadre and is responsible for ensuring trainers instruct trainees. They also ensure standardization, and monitor resource issues that affect their cadre’s training. It’s a new duality for squadron commanders, who must ensure effective training not only within their squadron, but also their assigned cadre.

The other major initiative improves schedule predictability for group events in order to more ef-



Photo by Staff Sgt. Kenneth Goss
Airman Chad Maurice assists with erecting a tent he will work in as a help desk technician during combat deployment exercise Raging Bull, when the 34th Combat Communications Squadron ‘deployed’ to Fort Sill, Okla.

fectively schedule training. Merging squadron and group scheduling information into a single electronic calendar gives cadres and commanders unprecedented visibility. Cadres use the calendar to plan training events, and juggle trainers and equipment. Commanders use the calendar to make resource decisions that protect training from unplanned taskings.

Results of enacting these initiatives are clear. Squadron commanders, flight commanders, superintendents and work center supervisors coordinate closely to plan and execute training. Group leaders have visibility into schedules across the group, and work to de-conflict resources.

See 3RD HERD Page 15

UAVs play vital role for warfighter

Headquarters Air
Combat Command
Intelligence,
Surveillance, and
Reconnaissance
& DCGS
Maintenance Team
Langley AFB, Va.

Unmanned aerial vehicles such as Predator and Global Hawk play a vital role in gathering intelligence and providing surveillance and reconnaissance for the warfighter. These “eyes in the sky” allow continuous monitoring of activities in specific locations with low risk to personnel, and help ensure warfighters have data needed for time sensitive targeting, predictive battle space awareness, and precision engagement.

Air Force communicators play a significant role in the UAV mission. Since Predator and Global Hawk are unmanned, they’re inherently communications-dependent. With Predator, pilots on the ground fly the aircraft using communications links, while sitting in a relatively safe and comfortable ground station hundreds of miles from the action. Likewise, ground-based sensor operators use communications links to control sensor selection, look angles and area coverage. Communications is also used to downlink Predator sensor data to the ground station and disseminate data to intelligence imagery analysts. Similarly, Global Hawk is controlled with communications links, and the aircraft downlinks sensor imagery to its ground station using communications links. The communicator’s job is not done when the UAV ground station receives the sensor data. This data must be transmitted over communications links to decision makers and analysts at the various C2 and intelligence exploitation centers, including warfighters at the air operations center and imagery analysts at Air Force distributed common ground system locations.

When the Air Force was called on to deploy



Photo by Staff Sgt. Jeremy T. Lock

Electrical and environmental technician Senior Airman Brian Fox, 31st Test and Evaluation Squadron, Edwards AFB, Calif., refuels a Global Hawk during an exercise.

Predator and Global Hawk UAVs in support of Operation Enduring Freedom, the Headquarters Air Combat Command director of communications and information systems stepped up to the plate. HQ ACC/SC supported the efforts to request, engineer and implement C2 and reachback communications architectures to support these critical platforms. HQ ACC/SC played a key role in helping the Tasking, Processing, Exploitation and Dissemination Office and USCENTAF/A6 develop communications architectures to transmit signals from UAV ground stations to warfighters in the area of operations, and HQ USCENTCOM and intelligence imagery analysts in CONUS.

Transmitting Predator video and Global Hawk imagery halfway across the globe presents a significant challenge. The warfighter and intelligence analysts need high quality, near-real-time video and high-resolution imagery, which translate to high transmission data rates and a low tolerance for transmission errors. Transmitting real-time digital streaming video and complex imagery isn’t a simple feat over modern, terrestrial communications systems. Delivering these signals from UAV typical orbit areas in a war zone, over remotely-located theater-based communications systems, is

See **HAWK** Page 19

AWACS 'Sentry Comm' provides initial comm

By 2nd Lt. Kevin Grant
*AWACS Ground Communications
752nd Computer Systems Squadron
Tinker AFB, Okla.*

Events of Sept. 11 shook our nation and mobilized the U.S. military. Shortly thereafter, at Tinker AFB, the 552nd Air Control Wing and the world's premier command and control platform, the E-3 Airborne Warning and Control System aircraft began preparations to respond. Upon notification of deployment, the 752nd Computer Systems Squadron's ground communications section began palletizing their equipment. The section had performed well throughout numerous exercises and deployments, but this situation was entirely different. In addition to the primary mission of providing secure satellite voice communications between the deployed AWACS commander and his aircraft, they received notification that initial communications reachback would not arrive at the deployed location until weeks later. Reachback capability was critical for connecting deployed units with higher headquarters for communicating critical data messages, such as tasking orders and intelligence products. Without an air tasking order it would be impossible for AWACS crews and the joint forces air control commander to coordinate or execute organized and effective air operations.

Teamwork and partnership helped the 552nd's Sentry Comm team overcome and solve this critical communications problem. Working closely with the Air Combat Command crisis action team, joint command and control center, and 3rd Combat Communications Group planners, they identified three methods for initial data connectivity: secure Internet protocol router network through international marine satellite, secure fax through INMARSAT, and Hammer RICK ultra-high frequency satellite data transfers. Since the 752nd didn't have these capabilities in-house, ACC's communications and information directorate and the 552nd Computer Systems Group commander put the call in to the Air Force Communications Agency and the 3rd CCG, respectively, to assist during this deployment. AFCA's Hammer ACE team supplied the capability to use iridium and INMARSAT commercial satellite systems for secure communica-



Photo by Tech. Sgt. Cedric H. Rudisill

E-3D Sentry maintenance personnel from the 405th Air Expeditionary Wing discuss an electrical problem in the landing gear at a deployed location Jan. 5.

tions. SIPRNET was provided using an INMARSAT terminal, laptop and Fortezza modem. Secure voice and fax capabilities were provided through two INMARSAT phones and two iridium securable satellite phones. The 3rd CCG, or 3rd "Herd," also stationed at Tinker, provided a Hammer RICK UTC with secure point-to-point satellite data communications capability. The three AFCA Hammer ACE members and one 3rd Herd member integrated seamlessly into the Sentry Comm team and deployed along with the initial AWACS deployers.

Another challenge facing Sentry Comm was unknown quality and type of electrical power at the deployed location. Many of the team's data processing devices required standard 110 volt AC power and were also sensitive to "dirty," or varying, power. Fortunately, the team identified these

See **AWACS** next page

April 2002

3RD HERD

From Page 12

In the end, personnel avoid potential obstacles to receiving high quality communications training. The most important contribution we can make to the war against terrorism is to provide warfighters with combat communicators who have the best possible training. With continued leadership focus on training and functional cadres to ensure standards, quality, and continuity, the Herd is making it happen. Hooah!

Photo by Staff Sgt. Kenneth Goss

Staff Sgt. David Tomlin and Airman James Townes, 34th Combat Communications Squadron, run cable for the deployed operations site during a recent Raging Bull exercise.



AWACS

From previous page

requirements before departing and purchased sufficient power transformers and uninterruptible power supplies. Sentry Comm experienced far fewer computer failures, compared to other organizations at the deployed location, and was able to focus on the mission without worrying about repairing equipment.

In addition to the initial reachback challenge, the Sentry Comm team was notified that AWACS would arrive several days before their supporting unit type code personnel. The ability to regenerate and fly combat sorties would be limited without communications support. To fix the problem, AFCA's Hammer ACE developed a fly-away package consisting of an INMARSAT phone and secure fax, and two iridium phones to carry on-board an AWACS aircraft in the first wave, to provide secure data and voice capabilities upon arrival. Aircrews used this package to report their arrival to Tinker.

Upon arrival, Capt. Hugh O'Donnell, deployed AWACS A6 communications – computer systems chief, and his team established secure voice and data capability through INMARSAT within 10 hours. INMARSAT worked well with text e-mails, but large file transfers were slow due to the system's limited bandwidth. INMARSAT secure phone quality was great – similar to calling overseas from CONUS.

Not everything was perfect. There were drawbacks to using commercial satellite systems in a combat environment. INMARSAT was extremely busy on the first night of bombings. The team experienced random INMARSAT interference problems at night, limiting ability to make data connections. Secure phone calls through INMARSAT worked most of the time, although going secure with others in JTF-SWA was difficult. Iridium phones had marginally acceptable quality, required calls to be placed outside, and experienced difficulty going secure at times, but they accomplished the mission.

Captain O'Donnell and his Sentry Comm team also provided reachback for RC-135 Rivet Joint, NKC-135 Big Crow and KC-135 tanker units, and various ground-to-air radios and land mobile radios for the maintenance operations center, command post, fire department, flight physicians, and other support organizations.

Few units knew it would take two weeks for communications infrastructure to arrive and be set up. Careful planning and partnering with Hammer ACE and the 3rd CCG were critical to AWACS ability to launch more than 20 initial combat missions. Taking advantage of lessons learned from Operation Desert Storm, AWACS successfully established initial communications capability at a bare base, overcoming obstacles and avoiding use of in-theater airlift for air tasking order delivery. The team once again gave meaning to their motto: "Sentry Comm – Anytime ... Anywhere!"

5th CCG leads change in deployable comm

By Jim Binnicker
TDC Program Manager
Air Combat Command
Langley AFB, Va.

In the last two years, deployable communications has faced more changes than in the previous three decades. And the 5th Combat Communications Group, Robins AFB, Ga., has been leading the charge in that revolutionary effort.

“Tactical communications is changing dramatically,” said Col. David Schreck, 5th CCG commander. “Combat communications groups are at the forefront of incorporating that new technology as the Air Force continues to replace tri-services tactical communications equipment, or TRI-TAC, with more modern systems.”

The main harbinger of change is the theater-deployable communications initial communications access package, and its follow-on robusting capability known as tactical display device. The TDC package provides secure and nonsecure voice and data capability for about 1,500 deployed people. The TDD package adds capacity for another 1,500 people, and equipment to provide redundancy for maintaining a long-term deployed presence.

Even though the Air Force is moving to new technology, the 5th CCG continues to use legacy equipment. “There are many units, especially in other services, which only use TRI-TAC, and may not be moving to more modern equipment such as the TDC package for quite some time,” the colonel said. As the Air Force transitions, the group has to ensure units with older equipment can still communicate through networks established by the group’s communications experts. “The requirements for communications systems continue to change rapidly,” he continued. “The new equipment provides a lot of flexibility in meeting our customers’ requirements. Since the 5th CCG and our sister unit at Tinker have no fixed base mission – deployed communications is our job and what we train for – we’re leading the charge to determine how to best use new Air Force technology, while ensuring we can still integrate and deploy older systems.”

Colonel Schreck equates transition from TRI-TAC to TDC, to a fighter unit transitioning to a new airplane. “This is like the 1st Fighter Wing at Langley, going from the F-15 to the F-22,” he



Photo by Master Sgt. Michael A. Kaplan
Airman 1st Class Lucas Bullen, 608th Air Communications Squadron at Barksdale AFB, La., ensures hardware integrity on a quick reaction satellite antenna in preparation for Exercise Blue Flag 02-4 in February.

commented. “This is a new weapons system for the men and women in deployable communications.” A major difference, he mentioned, is when a fighter unit transitions to new equipment, their operators and maintainers no longer stay current on the older equipment. “We won’t have that luxury in combat communications. We’re required to have experts able to maintain and operate both legacy and newer TDC equipment.”

To deal with those changes, the group established a number of initiatives to enhance training and take advantage of the unit’s vast expertise. The group’s emphasis was in three primary areas: creating councils of experts, enhancing training plans and programs, and standing up learning centers.

The group established five functionally-orga-

nized councils: airfield operations, base-level systems, network systems, support functions and administration. “We wanted to bring together the group’s most experienced men and women to trade ideas and improve practices,” said Capt. Patrick Daniel, a member of the base-level systems council. “Instead of each of the four mission squadrons producing training plans and philosophies, we’re working together to make sure everyone has the same tools.”

The councils have been effective, according to the captain. “Bringing in perspectives of people with different experiences gave us a fantastic opportunity to build training plans and share expertise. For instance, one of the mission squadrons has been using TDC-ICAP for almost three years. We’ve been able to share that expertise with other units that are just getting the equipment.”

Information gathered through these councils helps build standardized training plans, according to Staff Sgt. Todd Krulcik, group education and training. About a year ago, the group set out to ensure each Air Force specialty had a revamped and standardized training plan, tracked and managed through the core automated maintenance system.

To create the training plan, education and training people rely heavily on expertise generated through the councils. “We’re incorporating unwritten wisdom that doesn’t come from a technical order, but from experience,” said Sergeant Krulcik. “These training plans are living documents. We add knowledge from successful experimentation, lessons from deployments and exercises, and even trainer innovation.”

As the training plans come into being, the group faces a larger challenge with deployable communications: equipment. When the group deploys equipment, it isn’t available in-garrison for training. “Right now, our squadrons don’t have enough equipment at Robins to ensure everyone can get training they require,” according to Billy Keith, group chief of engineering. The engineering flight is responsible for assuring mission squadrons share equipment remaining at Robins. One way they do this is through learning centers.

The group has two operational learning centers: the Network Learning Center and the Airfield Learning Center. Another in development is the Systems Learning and Integration Center. All have the same mission: Provide each group trainee hands-on experience needed to set up and main-

tain his or her equipment. The group has proved this process in the Network Learning Center, the oldest of the three.

“We’ve seen benefits through the NLC for some time,” said Colonel Schreck. “We’ve effectively trained so many people on building computer networks, it’s impossible to imagine the mission without the NLC. Even though the Airfield Learning Center hasn’t been established as long, we’re already starting to see payoffs. It was very effective when much of our airfield equipment was deployed. Now, as these systems come back, we can see even greater returns on our investment.”

The colonel has equally high expectations of the Systems Learning and Integration Center. “Right now, we have people returning from Operation Enduring Freedom who had to leave their equipment in-theater,” said the colonel. “We’ll have to use resources available in-house and through the SLIC to not only ensure they stay trained until we can get replacement equipment, but to also ensure all other squadrons get necessary training exposure. We’ll also be offering this training to units outside the 5th.”

These three areas – training plans, councils and learning centers – play a key role in the group’s future. They’re essential to integrate and implement the concept of operations for deployable communications. Bringing TDC and its robusting package to the warfighter means a great deal of change in how a deployable communications unit organizes and deploys, said Colonel Schreck. This includes how the unit prepares to deploy and even with whom it deploys. “In the past, we thought in terms of a package – a complete suite of equipment that accomplished one particular task. Since TDC is modular, we’re able to be very flexible and modify our network to meet customer requirements. It’s truly an exciting and challenging time.”

To help meet requirements for maintaining older equipment, the group is also developing new relationships with Guard and Reserve forces. “This year, the 5th CCG is affiliating with a Reserve unit – the reservists will work and train with us, as a total force,” the colonel said. “As we move fully into integrating TDC, they’ll perform a critical bridging mission between TDC and our legacy equipment. The men and women of the group, and in the Reserve, are all looking forward to opportunities offered by this alliance.”

See **CHANGE** Page 19

ACC postal supports Enduring Freedom

By Capt. Daniel Leos
ACC Postal Services Flight Commander
83rd Communications Squadron
Langley AFB, Va.

Providing postal service in support of the war effort is no easy task. It seems postal is a facet of communications few really notice until the system is less than efficient or someone doesn't receive mail as expected. Establishing and overseeing postal service for Operation Enduring Freedom has provided many lessons learned that we can share with others for future contingencies.

About seven days after Sept. 11, the 83rd Communications Squadron's Air Combat Command Postal Flight learned postal troops were well on their way to Southwest Asia from another Air Force major command. Affectionately known as 8Ms, postal personnel were tasked to mobilize into SWA without ACC Postal's command and control. This was primarily due to the way the postal flight is aligned under ACC. U.S. Central Command Air Forces had no idea who we were and began critical postal planning stages on the time-phased force deployment data. This placed us in catch-up mode from the onset. For some of us in postal, this was our first experience with a real live war effort. It seemed like weeks before we could get the TPFDD process working properly to ensure the right people were sent to appropriate locations. The lesson learned here was to engage immediately with the unified command in charge to establish a conglomerate of key players to provide joint postal support and war planning.

After we were engaged in war planning efforts with U.S. Central Command and CENTAF, we confronted other challenges. As stressful as the TPFDD process was, we experienced great pains with communicating specific personnel line remarks, specifying proper rank and job skills necessary for each 8M duty position to CENTAF's joint operations planning and execution system. Because line remarks weren't specified initially, a core of young, inexperienced clerks was mobilized. Since line remarks are crucial when assigning resources for forward deployment, this process had some major kinks to be worked out.

Establishing 23 Army-Air Force post offices for more than 70,000 troops was a major milestone in itself. We couldn't request APO ZIP codes for con-



Photo by Staff Sgt. LeeAnn Sunn-Wagner

Staff Sgt. Matthew Lewis distributes mail in boxes at the Lajes Post Office, Lajes Field, Azores.

tingency sites because of classification issues. We had field commanders wanting mail for their people, yet we were unable to request ZIP codes until sites were declassified. The key is to get contingency sites declassified as quickly as possible without jeopardizing mission security. Requesting "Free-Mail" and addressing the issue of "Any Service Member" mail should also be done early in the operation.

Once APOs were established and mail was flowing to all contingency locations, our next challenge came from field commanders. Problems sprang up weekly from a variety of causes, such as transportation complications causing mail to be delayed or missing. Commanders called with postal concerns and wanted problems corrected immediately. We quickly learned communication was key, and it was

See **POSTAL** next page

POSTAL

From previous page

imperative to communicate early and often with commanders and customers about how the postal system worked. Commanders' expectations were understandably high for the sake of unit morale. However, since postal is an extremely complex and fluid operation, immediate fixes are often elusive at best.

Like the rest of the Air Force, postal is experiencing manning shortages, and we've had to rely heavily on the help of other MAJCOMs. Our limited ranks of experienced 8Ms are stretched even thinner by mobility rotations. Since the current war effort might not end for some time, the DOD Military Postal Service Agency may require MAJCOMs to pre-train 8Ms to operate all facets of postal, including logistics, transportation, operations and finance. With fewer seasoned NCOs available, more of our



Photo by Tech. Sgt. Scott Johnson

Senior Airman Rebecca Kanara, 65th CS postal specialist, places a letter from home into a customer's mailbox.

senior airmen and staff sergeants will be called upon to step into leadership roles to ensure continued operation of our contingency APOs.

HAWK

From Page 13

even more challenging. It took a combination of many different communications systems and a lot of hard work to pull this off. The OEF communications architectures used to support Predator and Global Hawk include commercial satellite, tactical microwave, terrestrial ATM, and trans-Atlantic fiber.

This isn't the first time HQ ACC/SC has been called on to support wartime UAV communications. Predator played a star role during Operation Allied Force operations in the Balkans. During this conflict, SC supported development of reachback architecture

to carry Predator video from the AOR to imagery analysts in CONUS, and developed tactics, techniques and procedures for restoring circuit outages and reporting circuit status.

There's a lot more work to be done. Global Hawk sensors can output imagery at higher data rates than currently implemented architectures can support. Predator video dissemination can be streamlined significantly by using direct receive satellite terminals, but we currently have only one in the Air Force inventory. HQ ACC/SC will be there to help implement and sustain solutions to these requirements and carry the torch into the 21st century.

CHANGE

From Page 17

With new equipment and partners, group leadership has been reviewing how to employ all aspects of deployable communications. Council members are providing a vast amount of advice and expertise to make combat communicators more effective. "Our experience with TDC ICAP has given us the capability to seriously consider how we set up and organize our equipment," said Captain Daniel.

"We learned a lot about using TDC during recent deployments for Operation Enduring Freedom," Colonel Schreck concluded. "Air Combat Command deployed five units equipped with TDC, including the 5th CCG's 51st Combat Communications Squadron. We learned a great deal about employing the new systems. To ensure we provide optimum services to our customers, we're taking those lessons, evaluating them in our councils, writing them into our training plans and teaching them in our learning centers. As we incorporate new weapon systems into the Air Force inventory, we know there will be some bumps in the road. However, as the face of deployable communications changes, the men and women of the 5th CCG are dedicated to making sure we change with it."

ACC meets challenges of C2 'sysads'

By Maj. Rob Robinson

83rd Communications Squadron
Langley AFB, Va.

One of the more exciting duty assignments available to Air Force communications warriors is to serve as a command and control "sysad," or systems administrator. At the cutting edge of direct warfighter support, the men and women who build, run and maintain our C2 systems possess tireless dedication, meticulous attention to detail, perceptiveness of a detective, and constant willingness to learn. For ACC-assigned C2 sysads, these are only some of the skills they bring to bear in working on components of the newest Air Force weapon system: the AN/USQ-163 Falconer air operations center.

In September 2000, Air Force Chief of Staff Gen. Michael Ryan designated systems and functions that make up an AOC to be an official weapon system. Prior to this, an AOC was simply a collection of stove-piped computer systems, with each functional area using a system that required a different set of skills to administer.

Formalization of the AOC as a weapon system is driving a change in the paradigm of how we conduct and support command and control. The Air Force is developing and maintaining a standardized baseline of a "system of systems." The first iteration, block 10, includes 46 separate components. This new way of looking at the AOC will provide more disciplined configuration control and allow for greater systems integration across areas of responsibility.

These 46 components are used in a variety of functional areas. Air Mobility Command uses the command and control information processing system as one of its mainstays to track various aspects of airlift. War planners use applications of the global command and control system to build and maintain operational plans and deployment data. Combat search and rescue uses personnel recovery mission software to track specialized rescue data. Weather professionals can login to a theater weather server to get the latest information on worldwide weather.

For ACC's combat air forces, the newest addition to the warfighters' C2 arsenal is an enormously powerful tool called theater battle management core systems. This collection of servers and client

workstations is the heart of the AOC's C2 engine.

Although each of these C2 tools is necessary to perform a specialized function, it's the *integration* of these disparate systems – actually making them share data with each other – that will be key to the new AOC and C2 paradigm. This integration will be accomplished not only by engineers and systems designers, but also the C2 sysads.

But just what are systems administrators and how do they help with integration? The sysad's role is often misunderstood not only outside the communications world, but by fellow communicators. Sure, they're the troops that unlock accounts, unfreeze applications, and "bring the system up" after a momentary shutdown. But sysads' skills and abilities are much more complex and involved in our Internetworked world.

Today's 3C0X1 C2 sysads spend most of their first year learning and internalizing the basics. Hours spent studying UNIX give C2 sysad warriors a foundation to begin learning system specifics, before attending specialized training. An example is the five-week basic TBMC course at the C2 Warrior School, Hurlburt Field, Fla. After graduating, sysads begin applying their knowledge to practice building the system, work through the 1,000-plus-page load summary, learn intricacies of data flows between servers, and troubleshoot the system to keep operators' clients running smoothly.

Besides the plethora of system acronyms, just what makes the C2 sysad's job so challenging? After all, isn't it just a matter of "point-and-click"?

Not at all. Most of the more powerful C2 systems run on large multi-processor, high-capacity-memory, UNIX-based computers. Machines with four or more 433 MHz processors and a gigabit of RAM are not uncommon, and systems administration is carried out with UNIX command line inputs. One mistyped command from a sysad with root access can bring down the entire system. When that system is being counted on by the three-star joint forces air component commander to plan, execute and monitor the day's air tasking order, you don't have the luxury of making a mistake – without the air tasking order, planes don't fly and bombs don't drop.

But being a sysad is more than that. These systems aren't worthwhile to warfighters without hard data: status of airfields, numbers of weapons, location and status of aircraft, and more. All

of this raw data is stored and manipulated through complex databases. To properly administer the databases, the C2 sysad also needs to learn some database administration techniques by attending even more specialized training courses.

A C2 system used to issue war orders must be completely secure. TBMCS, for example, uses various encryption devices, secure networks, firewalls, and virtual private networks. Each requires a different set of sysad skills, and few communicators have time to become an expert in all of them.

More and more components of major C2 systems are designed to be accessed using familiar Windows-based menus and Internet portals, Web-based protocols, and other Windows-based abilities, such as DNS, MExchange, and public key infrastructure. Since each of these skills takes months to learn and years to master, our blue-suit sysads seldom have continuing assignments that allow for the long-term building block approach necessary to develop into master C2 sysads.

Finally, all of the different C2 systems and servers within individual systems exchange data with each other using networked routers and switches. For C2 sysads to be truly valuable, they need at least a basic understanding of Internetworking theory, application and equipment. Completing basic networking computer-based training and classroom coursework is a good start, and a TBMCS sysad with network skills is a great asset.

Thus far, this article has covered C2 and systems administration, and briefly mentioned technical challenges, but the greatest task is personnel management and how we perform long-term systems administration.

As technology makes it easier for operators to use, systems behind the scenes are becoming more complex and requiring more in-depth training to maintain. Coupling this with retention difficulties, it's increasingly rare to find a 3C0X1 that has been able to stay with one C2 system for more than one assignment.

To maintain the level of knowledge and skills needed, the Air Force hires DOD-contracted civilians to bring highly specialized technical abilities to the table. In addition, our civil service civilians are employed to great effect in the C2 arena, bringing specialized abilities and long-term stability to the work center. Many civilians are deployable, just like blue-suit military, and have gone to forward locations supporting Operations Southern Watch and Enduring Freedom.

Although I've referred to the phrase "C2 sysad"



Photo by Staff Sgt. Greg L. Davis

OPERATION NOBLE EAGLE -- Portrait of a F-16D crewmember seen while in a turn during a combat air patrol mission in support of Operation Noble Eagle. He's assigned to the 20th Fighter Wing based at Shaw AFB, S.C.

throughout this article, there is no such specialty shred-out or Air Force specialty code. Our blue-suit C2 communications warriors are still generalists, and will probably be required to learn a new set of skills at each assignment. As a result, we not only lose training dollars and time spent on that individual, but must start again with the replacement.

Now is the time to consider a change in our processes. Perhaps we should develop more specialized AFSC tracks that will allow us to grow and maintain a deeper level of expertise. Perhaps we should apply special experience indicators and send our airmen to new assignments in similar C2 support jobs to continue building on hard-won skills. Perhaps we should develop a model based on aircraft maintenance and apply it to the communications arena.

Of all the challenges I've outlined here, the toughest is refining and applying the best, most efficient way to manage our people and skills in an expanding world of increasingly difficult and narrow technical focus.

The future of C2 systems administration is changing as the concept of the AOC as a weapon system develops, and systems complexity will continue to challenge our people by requiring higher levels of technical prowess.

Nevertheless, with a combination of civilian and military support, the Air Force communications warrior will be there to meet the challenge – whenever and wherever the need arises.



Remanence security essential to protect electronic information

By Col. William T. Lord
Director of
Communications and
Information
Air Mobility Command
Scott AFB, Ill.

Air Mobility Command is proud to join our partners from Air Force Special Operations Command in Information Assurance Campaign 2002 to cover topics relating to remanence security. Remanence security includes protecting systems and media being discarded, as well as properly sanitizing systems and media that have processed or inadvertently received transfers of classified information.

Typically, few people are aware of how much information might potentially be provided to unauthorized personnel by failing to properly clear or destroy magnetic, optical or other sensitive media. For example, somebody purchasing excess computers at the Defense Reutilization and Marketing Office may really be searching for sensitive residual information on those systems. Additionally, somebody dumpster-diving for diskettes or old hard drives may be hoping to

find operational details of our activities.

With such alarming possibilities, we need to intensify our efforts to ensure that any form of classified media is properly sanitized or destroyed to prevent giving any valuable information to America's enemies. Recent world events have exposed terrorist sleeper cells that patiently gathered information and waited for the right opportunity to execute their plans. In light of those re-

“Typically, few people are aware of how much information might potentially be provided to unauthorized personnel by failing to properly clear or destroy magnetic, optical or other sensitive media.”

Colonel Lord

cent attacks against America, we each need to be a little more cautious of how we protect our sensitive or potentially sensitive information.

Together, AMC and AFSOC have prepared the following articles for this issue of *intercom* to help teach those who support the Air Force mission that their role in remanence security is critical in maintaining a strong Information Assurance posture. Each Air Force team member must realize that it's important not only to protect information on our networks, but to use only approved products and methods to eliminate all traces of residual information on systems or media being disposed of or reused.

Don't make classified remanence the bad guy's 'gold mine'

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

Imagine the shock of finding an entire box of old unlabeled hard drives stashed in a supply closet, and then learning they contained classified or sensitive information. This recently happened to a fellow member of the Department of Defense. The problem in this case was the lack of remanence security. “Remanence?” you may ask. “What’s that?”

Information Assurance personnel from Air Mobility Command and Air Force Special Operations Command have joined forces in this issue of *intercom* to tackle this difficult subject. Remanence security is designed to ensure residual information can't be extracted from any media, such as floppy, hard and optical disks; disk packs; PCMCIA cards; toner cartridges; or printer ribbons. Remanence security is achieved through methods such as degaussing, over-

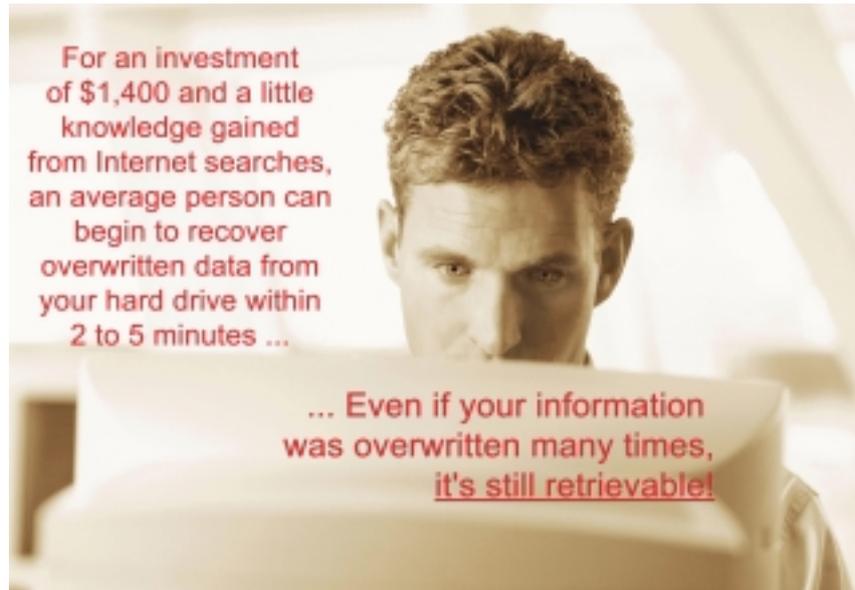
See **GOLD MINE** next page

An ounce of prevention simplifies remanence security

By Senior Master Sgt. Alan
McClellan

AMC Communications Group
Air Mobility Command
Scott AFB, Ill.

For an investment of \$1,400 and a little knowledge gained from Internet searches, an average person can begin to recover overwritten data from your hard drive within two to five minutes. Even if your information was overwritten many times, it's still retrievable. So how easy might



See **PREVENTION** Page 29

GOLD MINE

From previous page

writing and destruction. Remanence security is critical to security, because any residual image or information remaining on unprotected disposed media may unexpectedly give away important classified or sensitive information.

Although generic Air Force guidance on remanence security can be found in Air Force Special Security Instruction 5020, even IA experts can stumble when questioned on specific requirements. For example, the instruction requires destruction of computer monitors when images of classified material have been burned into the screen, yet specific procedures have never been spelled out. For working monitors, one approach is to try to "burn out" images by turning the intensity up and leaving it on until nothing can be read. Consequently, you must coordinate with safety personnel before destroying any potentially dangerous item.

Another example of general guidance from the AFSSI is the requirement to use Air Force approved disk-wiping software to sanitize magnetic media. Although DOD has identified software packages that meet its requirements, you must also assure the software has Air Force approval before using it. Software may be approved with local evaluation, by contract or Air Force review, and

with concurrence of the designated approval authority. Future commercial software will be assessed using NIAP common criteria.

Although closely related to full disk wipes, an important area not directly addressed by Air Force or DOD published guidance is an approved method for partial disk wipes for systems inadvertently contaminated by classified information. An example of inadvertent contamination is sending classified information from one unclassified computer to another. In this case, contamination would involve not only the two computers, but every relay point between the two systems. In order to minimize mission impacts, we can't always take all affected equipment offline and completely delete all e-mail, so partial disk wipe procedures must be developed and used.

This article has outlined some pertinent points covered by AFSSI 5020, to help you be better prepared to deal with remanence security issues. Policy continues to evolve, and an updated AFSSI 5020 is currently in coordination. In the meantime, your wing IA office is your best source for remanence security guidance. Any questions they can't answer may be referred to their MAJCOM IA policy office.

Remember, "One person's trash is another person's treasure." Just be sure you don't let your "classified remanence" become the bad guy's "gold mine"!

Remanence security needs your help

By Staff Sgt. Michelle Wellman
16th Communications Squadron
Hurlburt Field, Fla.

“The American people, our forces abroad and our friends and allies must be protected against the threats with which modern technology and its proliferation confront us,” according to Secretary of Defense Donald Rumsfeld.

We can no longer ignore real threats that should be one of our highest priorities. We must make a commitment to protect the information that keeps our nation strong. Make no mistake, Information Assurance and security are everyone’s responsibility.

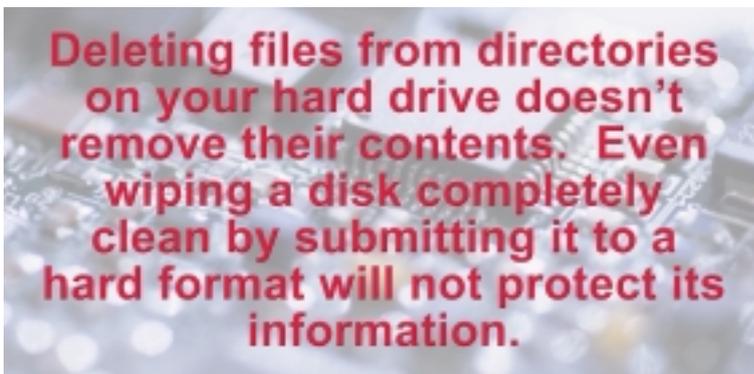
Sooner or later, all classified materials in an organization are either transferred or destroyed. Unfortunately, destruction often happens later, rather than sooner. People sometimes tend to hold on to classified information for no good reason. Destroying it when it’s no longer needed should be at the top of everyone’s priority list. After all, each item destroyed is one less to worry about.

Since you may be required to deal with classified or sensitive information at any time, you need to be aware of important issues accompanying that responsibility. This is where remanence security comes into play.

Remanence security involves effectively using proper methods to sanitize your magnetic media. Magnetic media includes any device that can store and maintain information. Understanding that concept can greatly reduce chances of a security incident.

Do you really know what’s on your hard drive? You need to be aware that it possesses retentive properties that cause data to remain, even after you may think you’ve erased it. This is referred to as data remanence, which is the residual physical representation of data that has been in some way erased or cleared.

What does clearing your hard drive do? Clearing is nothing more than removing data from a storage device in such a way that the data may not be reconstructed using common system capabilities. Notice I said, “common system capabilities.” This refers to such things as simple keyboard strokes, which don’t prevent data from being reconstructed using laboratory methods. Cleared media may be



reused at the same classification level or at a higher level. A common clearing method is overwriting.

If you’ve used these procedures to wipe classified or sensitive information from your hard drive, I have some bad news. The data is still there! Deleting files from directories on your hard drive doesn’t remove their contents. Even wiping a disk completely clean by submitting it to a hard format will not protect its information. What may appear to be a clean disk may in fact contain a wealth of information.

The second method commonly used to remove data from a magnetic media is sanitizing. This process assures information is unrecoverable by technical means. It includes removing all classified labels, markings and activity logs.

Purging is another way to sanitize hard drives and magnetic tape. This involves removal of data from a storage device in a way to provide assurance, proportional to data sensitivity, that the data can’t be reconstructed through open-ended laboratory techniques. The important thing to remember in this scenario is the storage device must be disconnected from any external network before purging.

There are two approved methods to ensure your hard drive has been sanitized – that all data has been erased and is unrecoverable. The first is a degausser, which is basically a large magnet. The degausser magnetically erases data from the magnetic media. Degaussing is acceptable and effective for sanitizing tape, diskettes, removable media and fixed hard drives removed from the unit. It’s important to assure the degausser performed as expected and data can’t be recovered. If a degausser isn’t available in your unit or on your base,

See **HELP** next page

What to do if you find classified info in your e-mail

Information Assurance Office
Air Force Special Operations Command
Hurlburt Field, Fla.

“NCC help desk, Senior Airman Smith, this line is unsecure. May I help you?”

“Um, yes, this is Joe Computer User, and I think I might have something classified in my e-mail.”

This is one nightmare your network control center hopes to avoid – having classified information on an unclassified network. Fortunately, NCCs have checklists, procedures, operating instructions and action plans for dealing with this situation. But what about Joe C. User? What part does he play?

Fortunately, User received Information Assurance training prior to gaining access to the network. Among other things, the training included remanence security, which is covered by AFSSI 5020, *Remanence Security*, and AFSSI 5021, *Time Compliance Network Order Management, and Vulnerability and Incident Reporting*. The official purpose and intent of remanence security is outlined in the AFSSIs, but the

bottom line for User and all of us is to protect sensitive information – both classified and unclassified – from persons lacking proper clearance or need-to-know. So User knew he had to call someone, but is that all he should do?

Some procedures vary from base to base. For example, the established procedure at User’s base might have been to call his work group manager, who would contact the NCC. At the very least, User should know and follow instructions he received in IA training.

As soon as he discovered the e-mail, User referred to his base’s customer checklist. First he disconnected his computer from the network, but didn’t turn the system off. He didn’t remove the diskette he was using or close out his e-mail. He noted the classification of the document, the originator – including name, unit and base – the message subject, and the names of the two attachments. After calling the NCC, he guarded his computer and disks until his WM came to help him.

The WM had her own list. She noted what actions User had taken, then contacted the NCC and her security manager. When classified information is sus-

pected to be on an unclassified system, it’s a potential security incident and may require investigation by security forces information security personnel.

After all was said and done, it turned out the message originator had decided to downgrade it to unclassified. Had it remained classified, the NCC could have faced hours of scrubbing servers to remove all traces of the message and attachments, and User’s computer would have had to be sanitized, or wiped clean, to ensure all classified data was removed from the system. No base enjoys downtime required to deal with this kind of situation, and no customer relishes the thought of having to wipe their hard drives and disks.

User doesn’t know what happens in situations like these, aside from what he personally experienced. For his part, he knew he had to do something, even if it meant he couldn’t use his system or his e-mail for awhile.

Do you know what actions you would need to take if this happened to you? To find out, contact your WM or your wing IA office. Do your part to keep our information secure.

HELP

From previous page

you may mail your hard drive to a location that has one, following procedures noted in AFSSI 5020.

The second method is to use Department of Defense and Air Force approved overwriting software. The Air Force posts reports on this software on the Air Force Information Assurance Web page. The list isn’t all-inclusive, so other software may be added in the future. More information is available on the Air Force Information Assurance Web page: https://www.afca.scott.af.mil/ip/info_services/product_sec.cfm?ProdID=3, or from

your local Information Assurance office.

Learning to properly sanitize magnetic media – such as floppies, hard drives and zip drives – is a necessity, and mandatory on military installations. It’s important to remember you may have classified or sensitive information on your hard drive. Would you want to give an unscrupulous person access to that information?

Information Assurance is an important aspect of military defense strategy that encompasses every Air Force mission. The Air Force needs your help to assure the security of its information systems.

Properly disposing of electronic data is vital

By Master Sgt. Keith Lefevre
16th Communications Squadron
Hurlburt Field, Fla.

Data remanence is the residual magnetic or electrical representation of data that's been in some way erased or overwritten. This residual information may allow data to be reconstructed, typically using time-consuming methods. This is normally only a concern to anyone processing classified information. For the unclassified community, overwriting of media is usually sufficient to reduce threat of reconstruction from data remanence.

To remove all data from storage media so that it can't be retrieved is called sanitization. Sanitization must be considered when media is transferred from one organization to another, equipment is declared surplus, or an organization disposes of media. Sharing of media within the government, or between government and contractors, also presents security issues or risks.

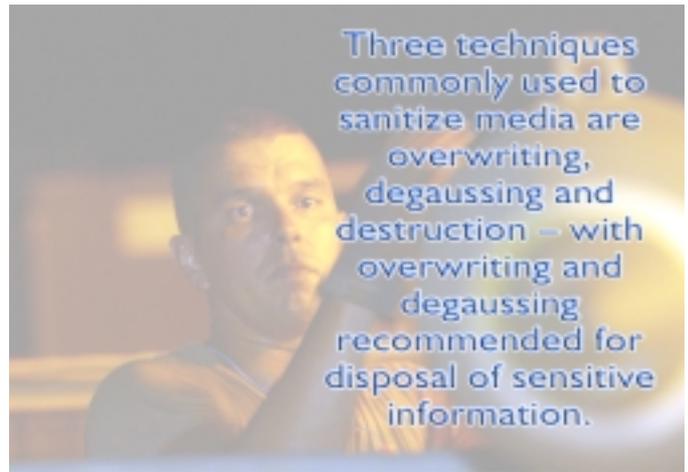
Another risk is when an employee throws away old diskettes believing that "erasing" the files has made the data irretrievable. Erasing the file simply removes the "pointer" that tells the computer where the file is located. The file may still be there. By using a utility program, available as off-the-shelf software, this "deleted" information can often be retrieved.

Proper disposition of sensitive data can be assured by establishing policies and procedures that consider the following factors:

* Magnetic media may be exposed to unauthorized access at various times in the system life cycle. When are exposures most likely to occur? How do they occur? What types of data are at risk? What procedures are appropriate for disposal of media for the specific operating environment?

* Contractors typically use their IT systems to process information owned by a federal agency. Are policies or contractual mechanisms in place to adequately protect this information? Contractors must be aware of the importance of implementing appropriate sanitization policies and procedures. Binding contractual provisions are often appropriate to ensure protection of the agency's information.

* The computer security training and aware-



ness program can be an effective mechanism to address media disposal and sanitization issues. Users require specific guidance and a source of answers to their questions.

* Is there leased equipment? If so, and it's used to process sensitive information, it must not be returned to the vendor until it's sanitized.

Three techniques are commonly used to sanitize media – including overwriting, degaussing and destruction – with overwriting and degaussing recommended for disposal of sensitive information.

Overwriting is an effective method of clearing data from magnetic media. Overwriting uses a program to write – for example, 1s, 0s, or a combination of both – onto the media where the file to be sanitized is located. The number of times the media is overwritten depends on information sensitivity. Don't confuse overwriting with deleting the "pointer" to a file, as discussed earlier. Inclusion of overwrite capabilities should be considered at the outset when designing sensitive applications.

Degaussing magnetically erases data from magnetic media. There are two types of degaussers: strong magnets and electric degaussers. Degaussers are tested by the National Security Agency for compliance with Department of Defense erasure requirements. Those that comply are placed on the degausser products list in the National Security Agency's information systems security products and services catalog. Common magnets – for example, those used to hang a picture – are relatively weak and can't effectively degauss magnetic media.

Destruction of media is another sanitization method. For specifics, consult AFSSI 5020 or contact your wing Information Assurance office. Shredding diskettes, after removing the outer pro-

See **DATA** next page

Following procedures assures remanence security

By Master Sgt. Greg Potts
16th Communications Squadron
Hurlburt Field, Fla.

The first step in achieving effective remanence security is to understand its definition. Magnetic remanence is the magnetic representation of residual information that remains on automated information systems' storage media after it's erased. Remanence security is use of prescribed safeguards and controls to prevent reconstruction or disclosure of sensitive information. All Air Force personnel must prevent accidental disclosure of this information. To do this, they must be knowledgeable of clearing, sanitizing and destruction procedures, and have the tools available to assist them.

Responsibility for remanence security resides at three levels:

- * The designated approving authority okays procedures for clearing, sanitizing and destroying storage media.

- * The wing information protection office maintains data on approved disposal resources and guidance.

- * The information systems security officer provides information on remanence security to users, operations personnel and approving authorities, to help them make informed remanence security decisions based on known risks, regulatory requirements and established procedures.

Procedures for clearing, sanitizing and destroying various types of storage media are outlined in AFSSI 5020, *Remanence Security*, chapter 3. The following criteria apply to each method:

- * **Clearing** removes information from storage media in a manner that renders it unrecoverable by normal system utilities or non-technical means. Clearing can be used when the secured physical

environment where the media exists is maintained. The following guidelines apply to clearing:

1. Clear storage media when changing modes of operation or prior to reuse at higher classification level.

2. Clear storage media containing sensitive information before reuse or release from Air Force control.

3. Ensure markings for the highest processed classification remain on the media. Use a Standard Form 711 to annotate in the comment block the media is cleared. Also include the date and agency clearing the storage media.

- * **Sanitizing** removes sensitive information from storage media in a manner that assures data is unrecoverable by any technical means. Some examples of appropriate situations for use of sanitization are:

1. When the secure physical environment where the media was used will not be maintained.

2. When the media will go from a secure to a non-secure facility.

3. When the media is inadvertently exposed to a higher than allowed classification or category of data.

- * **Disposal** of storage media is authorized after sanitization, in accordance with local destruction procedures.

Questions on local sanitization, destruction and disposal methods should be directed to your wing Information Assurance office.

Remanence security is everyone's responsibility and isn't a matter to be taken lightly. It ties directly to protection and safeguarding of sensitive information.

Additional information is available from AFSSI 5020, *Remanence Security*. Contact your information protection office for detailed local guidance.

DATA

From previous page

tective casing, is an option for unclassified media.

When developing a sanitization program, it's important to keep some essential elements in mind:

- * Media containing sensitive information should not be released without appropriate sani-

tization.

- * File deletion functions – for example, the Delete command on MS-DOS – can usually be expected to remove only the “pointer” to a file, rather than the file itself.

- * When data is removed from storage media, every precaution should be taken to remove duplicate versions that may exist on the same or other storage media,

back-up files, temporary files, hidden files, or extended memory.

- * Media in surplus equipment should be sanitized.

A copy of the current degausser product list is on the Air Force IA Web page: <https://www.afca.scott.af.mil/ip>, under *Info and Services, Product Assessment, Degausser and Destruction Device Lists*.

Scenario tests remanence security

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

Have you ever wondered what might happen if an individual took classified, or sensitive unclassified, information home on a disk, then used their home computer and personal e-mail account to forward that information to others? While this situation might at first sound hypothetical, it's actually happened. What actions are required in such a case to try to keep that information from falling into the wrong hands? What security disciplines are involved? What are the potential impacts on the Air Force?

The first thing that should happen is to notify the individual's supervisor, commander, security manager and servicing network control center. The security manager will initiate actions required by AFI 31-401, *Information Security Program Management*, and prepare and coordinate an incident report with the commander and security forces squadron. The network control center, or network operations support center, will immediately take actions required by Air Force Special Security Instruction 5020, *Remanence Security*, or procedures approved by the network designated approving authority to clear network mail servers and other computers of sensitive and classified information.

Before proceeding, it's important to note there's no canned answer on how to handle these incidents. The network DAA, usually at wing commander or major command level, determines the appropriate response. Among issues each DAA considers is risk to national security posed by the compromise, capabilities and trust in sanitization tools, including file or disk wipe software, and impact on individuals due to loss of personal data.

In this scenario, you might think it would also be a good idea to clear hard drives and other com-

puter media of all affected personal computers and workstations. AFSSI 5020 provides guidelines for sanitization that must be used in the absence of DAA approved procedures. Normally the security manager or a workgroup manager assists to ensure proper sanitization of hard drives – including those in private residences. Your servicing Information Assurance office can also provide guidance as needed.

As you can imagine, sanitizing computers, disks and other media of everyone involved is possible, but it can be extremely difficult to identify every system on the Internet that received the information. The situation is further complicated if recipients forwarded the message to more individuals. The problem could be compared to dropping printed messages from an airplane over a city, then trying to recover every copy of the message before it's read. In some cases, the Air Force should request assistance of federal law enforcement agencies, such as the FBI.

For sanitizing magnetic computer media, AFSSI 5020 approves two methods: degaussing, and overwriting multiple times with software meeting DOD and Air Force requirements.

To degauss hard drives or other magnetic media, they must first be removed from computers and subjected to magnetic fields strong enough to eliminate traces of sensitive or classified information. Degaussing equipment must meet National Security Agency standards. A hazard associated with degaussing is the possibility timing marks on hard drives may be erased, rendering the drives useless.

To sanitize with software, you can locate approved computer programs on the Air Force Information Assurance Web page, or in Attachment 2, Page 7, of the Assistant Secretary of Defense Memorandum of June 4, 2001. Regardless of



See **SCENARIO** next page

SCENARIO

From previous page

method used, each sanitized hard drive must be labeled with date, time and signature of the person accomplishing the procedure. Figure A-3.1 of the memorandum gives label requirements.

Now more than ever, it's imperative for personnel who deal with sensitive or classified information to review and follow protection procedures specified in applicable Air Force instructions. This approach will help decrease the likelihood of similar incidents.

Each Air Force team member must understand that remanence security is most useful when all affected computers can be identified, but when information is sent by e-mail over the Internet it may not be possible to eliminate every trace. The security breach caused by sending classified information over unclassified systems can seriously dam-

age national security. So be sure you know and follow proper procedures for protecting sensitive and classified information.

For more information, consult the following links: Air Force Instruction 31-401, *Information Security Program Management*: <http://afpubs.hq.af.mil/pubfiles/af/31/afi31-401/afi31-401.pdf>

Air Force Special Security Instruction 5020, *Remanence Security*: <https://www.afca.scott.af.mil/ip/pdf/5020.doc>

Air Force Information Assurance Web page, *Remanence Security*: https://www.afca.scott.af.mil/ip/info_services/compusec_sec.cfm?COMPID=6

Assistant Secretary of Defense Memorandum, June 4, 2001: https://www.afca.scott.af.mil/ip/info_services/compusec_docs/ASD_HD_Disposition_memo060401.pdf

PREVENTION

From Page 23

it be for a skilled foreign intelligence agency to recover your "sanitized" data? Hopefully this article will shed some light on good remanence security procedures to help you better protect sensitive and classified information.

Effective remanence security promotes removal of all traces of information from disk drives to prevent compromise of sensitive or classified information. Air Force Special Security Instruction 5020 provides user guidance for removing traces of information from disk drives, diskettes, tapes and other electronic storage media.

The Internet has a wealth of information and tips for recovering overwritten data. I researched companies claiming to be able to recover deleted or overwritten information from hard drives. I learned most of them could easily restore deleted infor-

mation, or recover information from physically damaged hard drives. Surprisingly, most companies couldn't recover information from hard disks that had been overwritten. This led me to believe software overwrite procedures might be adequate for security.

I tried a different Internet search approach and found enough information to scare any security manager. I learned overwrite software may not be adequate, because hard drives leave more than enough room for each bit to be stored. As a result, hard drives seldom record bits of information in exactly the same position as previous information. An analogy is stacking cards and slightly shifting each new top card to one side or another. As a result, sophisticated equipment can analyze layers of previously recorded data to find information thought to have been overwritten many times. Although most equipment used for this purpose is expensive, devices can be built

for approximately \$1,400 using an average personal computer.

Before I share with you my ultimate remanence security tip, here are a couple of other ways to protect sensitive or classified information. First, don't heat magnetic computer media – for example, by leaving a laptop in a hot car – because it will make it much more difficult to permanently erase information later. Second, the longer information is stored on magnetic media, the more difficult it is to erase later, especially for your computer RAM chips.

Last, the most important advice of all: If you never put sensitive or classified information on an unclassified computer, you'll never have to worry about trying to clean it off.

For more information on remanence security and degaussing software, go the Air Force Information Assurance Web page, <https://www.afca.scott.af.mil/ip>, and see *Info & Services, COMPUSEC Info*.

Retired comm leader dies at age 66

SEATTLE – A retired Air Force communications leader, Lt. Gen. Robert H. Ludwig, 66, died March 4 of cancer, in Seattle.

The career communicator served as deputy chief of staff, command, control, communications and computers, Air Force headquarters, at the time of his retirement on June 1, 1992.

He was commissioned through the Reserve Officer Training Corps in 1958, and completed the communications-electronics officer course at Keesler AFB, Miss., a year later. He served in communications assignments around the globe, including California, Japan, Nebraska, Taiwan, Missouri, New Mexico, Maryland and Alaska. He commanded the Pacific Communications Division from 1982 to 1984, and the Strategic Information Systems Division from 1984 to 1986.

He became assistant chief of staff of systems for command, control, communications and computers, Air Force headquarters, and three years later he commanded Air Force Communications Command, Scott AFB. In 1990, he took his final assignment as deputy chief of staff for command, control, communications and computers, Air Force headquarters. When this position was created, he became the first to hold that office, and the first three-star to lead the communications community.

An impressive record of accomplishments by Air Force communicators during those years serves as a tribute to his leadership. The Air Force took a step toward the future when it established the Computer Systems Division at Gunter Annex, Maxwell AFB, Ala., in 1989. It was responsible for acquisition policies, long-range planning, and programming for future standard communications and computer systems. Major acquisitions, such as the base information digital distribution system, and the cargo movement operations system, supported DOD activities worldwide.

General Ludwig often talked about the Air Force's evolution toward more computer networking. Consistent with his vision, the Standard Systems Center introduced a computerized base-level personnel system to the entire Air Force, and modernized base service stores and tool issue centers by introducing a system that used microcomputers and bar code technology.

The general guided AFCC through the defense



Lt. Gen. Robert H. Ludwig

management review process that resulted in a major reorganization of the command, as its operational and maintenance functions were transferred to the major commands. AFCC supported all Air Force operational and support commands by providing communications, computer and air traffic services. The command acquired, engineered, installed, operated and maintained these services.

The AFCC enlisted corps honored General Ludwig by inducting him into the Order of the Sword in 1991.

After retiring in 1992, General Ludwig continued public service through the Air Force Association, Armed Forces Communications and Electronics Association, and Air Force C4 Association.

General Ludwig was born Feb. 9, 1936, in Minneapolis. He is survived by his wife, Nancy, and four children.

Funeral services were held March 7 at Tahoma National Cemetery, Kent, Wash.

Contributions may be sent to the Air Force Command and Control, Communications and Computers Association (AFC4A), 11402 Meade Pointe, Fawn Lake, Spotsylvania, VA, 22553-4616, or to the Bob Ludwig Scholarship Fund, Air Force Communications Agency Booster Club, 203 W. Losey St., Room 1010, Scott AFB, IL, 62225-5222, (618) 229-6007 or DSN 779-6007.

Initiative reduces airfield obstructions

TYNDALL AFB, Fla. – A tragic mishap claimed the life of an Air Force pilot in July 1998, when his aircraft departed the end of the runway after an aborted takeoff and collided with some infrangible -- or unbreakable -- structures. The mishap drew the attention of the Air Force chief of staff, who directed corrective action. As a result, an Air Force-wide data call was issued to identify all such airfield obstructions that presented a potential hazard to flying operations. Air Force headquarters assembled a cross-functional tiger team to investigate causes and make recommendations.

First, the team collected, collated and analyzed data submitted by bases to frame the issues. Then it hosted a workshop for approximately 40 experts from various disciplines to gain more insight. Results were documented in a Nov. 27, 2000, Airfield Obstruction Reduction Initiative Report.

The team's three objectives were to evaluate the Air Force inspector general's recommendations; survey the Air Force and establish a funding strategy to help remove existing obstructions; and recommend policy and procedural changes to prevent new obstructions being placed too near airfields.

SAF/IG recommendations were validated through data review and discussion with experts, and then details were developed to implement change. The first recommendation was to adopt the Federal Aviation Administration's specification for low impact resistant structures. Although the Air Force had adopted this specification, it had only been applied to airfield approach lights. As a result, language was expanded to address application of the specification to other systems and structures, and to define the minimum area of frangibility on an airfield. The new standard is described at Attachment 1 to the AORI report and will soon be included in a change to Air Force Manual 32-1123.

The second SAF/IG recommendation was to ensure leadership within all civil engineering units understood and complied with frangibility requirements. Several actions are pending to address this recommendation. In February 2001, Air Force headquarters issued a policy memorandum requiring all airfield-related projects to be coordinated with airfield management, safety, communications, community planning and design engineers. Guidance for the operations management field is being revised to include the requirement. More emphasis is being placed on frangibility issues in airfield management training, and Air Force Civil Engineer Support Agency is developing a CD-ROM training program for all personnel. The reliability and maintainability checklist for designers is being revised to include frangibility for airfield structures. AFCESA, in conjunction with the Engineer Research and Development Center and Lockwood Greene Technologies, is developing an engineering technical letter on standard frangible designs.

Another recommendation was that Air Force headquarters ensure major commands identified all infrangible structures within clear zones and made removal a priority. This aspect is addressed in the Funding Strategy section of the AORI Report. Bases identified all obstructions last year in the data call. The tiger team analyzed mishap locations and then developed an Air Force prioritization model. The tiger team's funding strategy was approved to add \$15 million each year from FY '03 through FY '10 as a "must pay" bill. Many other actions are being accomplished to aid this effort.

For more information, see the AORI report at <http://www.afcesa.af.mil>, or contact Mike Ates, AFCESA, at DSN 523-6351 or (850) 283-6351.

609TH

From Page 11

joint intrusion detection systems. Another measure was to use an open source IDS, Snort, which is a software-based real-time intrusion detection system developed by Martin Roesch, at Defense Information Systems Agency's de-

fense satellite communications system strategic tactical entry point sites. As a result, the theater saw no unauthorized access of its data networks at a time when hacker activity on the Internet was at an all-time high.

Prior to OEF, the 609th ACOMS received the Lt. Gen. Harold W. Grant award in 2000

for being the best small communications unit in the Air Force. Due to the squadron's professionalism and diligence, the C4ISR foundation was effectively laid, enabling success of OEF in Afghanistan. The 609th will continue the same level of commitment, wherever the war on terrorism may lead.

Air Force IT leaders receive recognition

WASHINGTON – Six Air Force information technology leaders were among 100 individuals recognized last month by *Federal Computer Week* for making a difference in federal IT in CY 2001.

Honorees included retired Lt. Gen. Albert Edmonds, Col. William Lord, Col. Thomas Verbeck, Master Sgt. Norman Cool, Gary Brooks and Mark Reboulet.

Winners were nominated by *FCW* readers, and selected by an independent panel of judges, for contributions to development, acquisition or management of federal IT.

According to the publication, the awards program is intended to give credit to those who had a significant impact on the federal IT community, rather than to be a popularity contest. Consideration is given to what nominees did, rather than the positions they held. Winners are considered to be part of an all-star team, rather than a hall of fame. Judges are picked from among the winners' peers, and include government and industry executives who displayed extraordinary effort and commitment in the previous year.

Lt. Gen. Albert Edmonds, Air Force retired, is president of Federal Government Information Solutions for EDS. General Edmonds lent his expertise to a multitude of associations, including the Armed Forces Communications and Electronics Association and the Information Technology Association of America, to help forge better working relationships between government and industry. He also oversaw a successful startup for deployment of the \$6.9 billion Navy Marine Corps Intranet, a groundbreaking system designed to tie together Navy operations.

Col. William Lord, director of communications and information, Air Mobility Command, Scott AFB, Ill., led AMC's e-mail, network and server consolidation initiative, now being emulated by other Air Force organizations. In 2001, he took command responsibility for Air Force consolidation efforts, including combining e-mail and network management services for 28,000 personnel at five bases in one location. This greatly reduced personnel and computer costs,

while maintaining responsive service.

Col. Thomas Verbeck, commander of the Air Force Communications Agency, Scott AFB, Ill., headed the effort to provide warrior-focused, mission-critical C4I support for the U.S. Air Forces Central Command initiative to relocate the Joint Task Force Southwest Asia Headquarters and Coalition Air Operations Center to Prince Sultan AB, Saudi Arabia, for Operation Desert Shift. He also led activities to provide special forces teams in Southwest Asia with command and control capabilities for Operation Enduring Freedom, including real-time targeting, battle damage assessment and force protection information.



Colonel Verbeck

Master Sgt. Norman Cool, superintendent of systems engineering, Air Mobility Command, Scott AFB, Ill., led AMC's information transformation and consolidated many of the command's applications, resulting in data that is better organized and more supportive of the command's mission.

Gary Brooks, chief of the plans, programs and requirements division, Air Force Materiel Command, Wright-Patterson AFB, Ohio, managed enterprise-wide initiatives undertaken by AFMC in 2001, including deployment of Microsoft Windows 2000 Active Directory for 40,000 users, which became the pilot program for Air Force-wide adoption. He also oversaw deployment of systems management tools to AFMC bases, which improved overall security and real-time control of AFMC networks; the adoption of collaborative tools; and the effort to define standards for server configuration and consolidation.

Mark Reboulet, program manager for the Automatic Identification Technology Program Management Office, Wright-Patterson AFB, Ohio, spearheaded wireless and bar code technology programs with such success that they were chosen to be deployed Air Force-wide, and other military services may follow suit. Programs included the standard asset tracking system's smart cards and warehouse management system, which reduced paperwork by 96 percent.



Colonel Lord

USTRANSCOM garners Rowlett award

WASHINGTON – A U.S. Transportation Command office has earned the National Security Agency’s top award for information systems security.

The Frank B. Rowlett Trophy for Organizational Achievement for 2000 went to the Information Systems Security Branch, of USTRANSCOM’s Command, Control, Communications and Computer Systems Directorate. Maj. Shari T. Miles, branch chief, accepted the award in February in Washington.

According to NSA, the award has been made annually since 1989 to the U.S. government organization making the most significant contribution to improvement of national information systems security, operational assurance readiness, or the defensive information operations posture of the United States. To earn the award, the branch competed with nominees from throughout the federal government.

“This award is truly an honor and testament to the hard work of our security staff,” said Major Miles.

“Securing USTRANSCOM’s information systems is a constant job, 24 hours a day, and this recognition is like winning a gold medal at the Olympics.”

In citing USTRANSCOM’s achievements, NSA noted the Information Systems Security Branch, “sustains one of the most advanced Information Assurance and information protection programs” in the Department of Defense.

The branch’s program is based on key success factors: people, technology, operations and training. It encompasses a wide variety of initiatives, from cross-trained computer security personnel, to advanced hardware and software security tools, to a flexible risk mitigation strategy.

“Our security staff members are experts in their field,” said Major Miles. The team has a mix of military, civil service and contractor personnel, the major said.

During the award period, USTRANSCOM’s Information Assurance and information protection program significantly elevated the standard of excellence for achieving operational IA readiness, and



Photo courtesy of Larry Bowers, NSA
Maj. Shari Miles, U.S. Transportation Command J6-OS, receives the Rowlett Trophy for Organizational Achievement from William B. Black Jr., deputy director NSA.

contributed to raising the bar for measuring superior defensive information operations in DOD. The Global Command, Control, Communications and Computer Systems Coordination Center gives USTRANSCOM’s key decision-makers vital information for assessing operational security of command and control systems. The GCCC presents a cohesive near-real-time enterprise-wide view of the C4S capability, and infrastructure supporting the defense transportation system.

USTRANSCOM’s IP program follows a strategy for risk mitigation by assessing cutting-edge products and standards. Capabilities established to support tactical IA/IP efforts include configuration management, firewall operations, proxy servers, intrusion detection, command-wide training, incident response, virus detection, auditing and vulnerability assessments.

Additionally, USTRANSCOM maintains a robust communications security monitoring and support program stemming from a number of vital initiatives. A proactive staff contributed to successful network connectivity of the Sensitive But Unclassified and Fortezza For Classified Certified Au-

See **ROWLETT** Page 34

Senior officers reassigned

Several moves were announced for senior communications and information officers.

Lt. Gen. Leslie F. Kenne will be reassigned from commander, Electronic Systems Center, Air Force Materiel Command, Hanscom AFB, Mass., to deputy chief of staff, Warfighting Integration, HQ U.S. Air Force, Washington.



General Kenne

Brig. Gen. Michael W. Peterson will move from director, Communications and Information Systems, HQ Air Combat Command, Langley AFB, Va., to commander, 81st Training Wing, Air Education and Training Command, Keesler AFB, Miss.

Col. William T. Lord, nominated for brigadier general, will go from director, Communications and Information, HQ Air Mobility Command, Scott AFB, Ill., to director, Communications and Information Systems, HQ ACC, Langley AFB.

Comm and info officer Web site hits the mark

By Laura Arzavala
Air Force Communications Agency
Scott AFB, Ill.

The Air Force communications and information officer home page has been up and running for a year. The site has logged more than 17,000 visitors, and user feedback has been outstanding.

The site provides a clearing house for up-to-date mission and career information and emerging technologies. The professional development area features career path guides for officers and civilians. The training areas have information on professional military education, chief information officer training, acquisition training, and education with industry opportunities. Unique to the site is a section for technical refresher training, with links to more than 400 online sources on various technologies, including the Air Force computer-based training site.

Since its opening, the site has

evolved significantly in response to user comments and suggestions. One adopted recommendation was to add a subscription function so users could sign up for automatic e-mail notifications to let them know when particular areas were updated.

Lt. Gen. John L. "Jack" Woodward Jr., Air Force deputy chief of staff for communications and information, praised the site and encouraged its use.

"As Air Force capabilities and commitments continue to expand, we need to ensure our comm and info professionals stay ahead of the curve," he said. "I believe we have a winner with our communications and information officer home page. I encourage all Air Force comm and info officers and civilian equivalents to use it to aid in daily mission requirements, as well as long term planning for a career as an Air Force communicator."

For more information, visit their Web site at <https://www.afca.scott.af.mil/33sx/>.

ROWLETT

From Page 33

thority Workstation systems. This milestone distinguished the command for having the first CAW site DOD-wide to achieve network connectivity with the directory server agent at Gunter Annex, Maxwell AFB, Ala.

USTRANSCOM also has programs under way to broaden impact of its IA efforts. By exchanging raw network data samples and research techniques, USTRANSCOM partners with NSA's Research and Engineering Organization in their intrusion detection research, and assists in evaluating information systems security capabilities. Additionally, USTRANSCOM effectively teamed with Defense Information Systems Agency to bring DOD services and products to augment commander-in-chief capabilities.

Two other finalists were recognized: the National Institute of Standards and Technology's Security Testing and Metrics Group, and U.S. Southern Command's Information Assurance Division. USTRANSCOM also received the award in 1997.

The award is named for Frank B. Rowlett, a renowned cryptologic pioneer who served as first commandant of the Central Intelligence Agency's National Cryptologic School.

Air Force unveils IT purchasing site

By Sally Wagner

Chief, Development & New Business Division
Standard Systems Group
Maxwell AFB-Gunter Annex, Ala.

Ordering and buying information technology products is being standardized for the Air Force with creation of a Web site called Air Force Way.

Air Force Chief Information Officer John M. Gilligan approved release of the program on March 1. A re-engineered process for procuring IT products, AFWay significantly improves approval procedures, enforces CIO standards, and ensures positive control and accountability for hardware and software prior to delivery.

Gilligan said AFWay provides standard, streamlined acquisition of IT solutions that conform to Air Force standards. Since the process is integrated with the Air Force IT inventory tracking system and information processing management system, it improves visibility and control for IT spending. Visibility is essential for informed IT investment decisions, and planning and budgeting deliberations.

“The Air Force has made a commitment to current Air Force IT vendors that the initial fielding of AFWay will not decrease their business opportunities,” Gilligan said. “The Air Force is working with current Air Force vendors, including those who supply individual major commands and bases, to include them as AFWay suppliers. Based on progress to date, moving existing contracts to AFWay is relatively easy.”

AFWay was built as a joint initiative between Air Combat Command and SSG, said Robert Frye, Standard Systems Group executive director. As lead command, ACC represents the needs of Air Force customers and will work with other MAJCOMs to ensure future releases of AFWay meet their needs. SSG serves as program manager, responsible for lifecycle management of the automated system, he said. “We’ll continue to negotiate and award contracts for the sale and service of IT products through the Commercial Information Technology - Product Area Directorate.”

Brig. Gen. Michael W. Peterson, ACC director for communications and information systems, said the most important aspect of AFWay is the opportunity to steer business re-engineering opportuni-



ties for Air Force expeditionary combat support. “AFWay enables near order of magnitude improvement over previous methods,” he said. “Tools like AFWay focus on improving processes – transforming the way we get things done, and ultimately leading to returning our airmen to their core competencies. The efficiencies AFWay creates apply directly to better manning, training and equipping of our expeditionary Air Force.”

ACC and SSG are also partnering to provide user training. The joint team is traveling to many MAJCOMs this month to ensure all users understand their role as they work within the AFWay business process. SSG and sponsoring MAJCOMs are also spending time with vendors to ensure their products are loaded and available for ordering.

Gilligan said the initial evaluation period for use of AFWay will focus on identifying and fixing any issues or problems. A key effort during this time will be to move existing contracts to AFWay. Another focus will be to ensure user needs are met by the re-engineered business processes for requirements definition, funds management, purchase approval and asset tracking.

As more IT purchases are made using AFWay, the Air Force expects to see a reduction in overhead and total Air Force IT ownership costs. AFWay will make the Air Force IT enterprise more easily sustainable and reliable through enforcement of standard IT solutions. In the coming months and years, the Air Force will use AFWay as a transformational tool to bring business process improvement to Air Force expeditionary combat support.

For more information, visit AFWay’s Web site at <https://afway.af.mil/>.

Joint Guardian

**Enduring
Freedom**

**Southern
Watch**



**Northern
Watch**

**Noble
Eagle**

Joint Forge

