

intercom

Journal of the Air Force
C4 Community

*AFRC
Comm and Info ...*



*... force provider
to the
force providers*

Air Force Chief of Staff
Gen. John P. Jumper

**Deputy Chief of Staff for
Warfighting Integration**
Lt. Gen. Leslie F. Kenne

**Deputy Chief of Staff for
Air and Space Operations**
Lt. Gen. Charles F. "Chuck" Wald

**Deputy Chief of Staff for
Installations and Logistics**
Lt. Gen. Michael E. Zettler

**Director of CAISR Infostructure
DCS for Warfighting Integration**
Maj. Gen. Charles E. Croom Jr.

**Commander,
Air Force
Communications Agency**
Col. David J. Kovach

Editorial Staff

AFCA Chief of Public Affairs
Lori Manske

Executive Editor
Len Barry

Editor
Tech. Sgt. Michael C. Leonard

Contributing Editor
AFRC/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.

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



Air Force Reserve Command comm and info

Reserve comm and info warriors meet needs of AEF Page 4
AFRC's comm and info director talks about the AFRC's comm and info mission.

Reorg postures comm and info for future missions Page 9
AFRC assessment identifies need to restructure comm and info function and organization at all levels.

Comm and info reservists support war on terrorism Page 17
Members of the AFRC comm and info team continue to play a major role in our nation's involvement on every continent, responding on short notice, exactly as advertised.



McGuire reservists spring into action Page 18
Following the Sept. 11 terrorist attacks, the 514th Comm Squadron, one of AFRC's Theater Deployable Comm units, supported two 90-day rotations via two 18-person global reach bed-down teams. This marked the first time the 514th CS was ever activated in its 20-year history.

4th Combat Camera Squadron plays key role in Millennium Challenge Page 22
March ARB's 4th Combat Camera Squadron participated in the Weapons Systems Video/Non-Linear Editor portion of the Millennium Challenge 2002 exercise. The war scenario was completely simulated using 51 simulators. There were 13,500 personnel involved at nine separate training sites in the continental United States.

in other news
New system makes tracking supplies easier Page 25

'Enterprise architecture'
Blueprint process brings together individual systems to form integrated capability Page 28

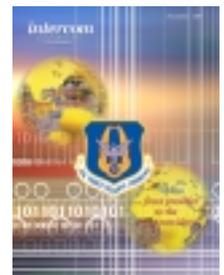
Information assurance campaign 2002
Information protection: Know user responsibilities Page 31

features
Celebration of comm heritage: AACS alumni meet in Dayton Page 36

Rohna: Communicator survived maritime disaster Page 38

On the cover

This month's cover focuses on Air Force Reserve Command's communications and information mission.



Cover by Tech. Sgt. Mike Leonard



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



Photo by Gary Ell

A McGuire AFB, N.J., KC-10A taxis down the flightline to a waiting crowd of family members and fellow reservists last November. Reservists were

returning to McGuire after spending a month overseas in support of Operation Enduring Freedom.

Reserve comm and info warriors meet needs of AEF

By Col. Richard M. Jensen

*Director of Communications and Information
Air Force Reserve Command
Robins AFB, Ga.*

Air Force Reserve Command is proud to be highlighted in this month's *intercom*. Since we don't have a large active duty presence, many *intercom* readers may be unfamiliar with AFRC. A quick, broad-brush introduction will put the rest of the articles in this issue in perspective.

Ever since our redesignation in 1997 as the Air Force's ninth and newest major command, we've occupied a unique niche in the Air Force and are faced with some novel challenges. We operate daily as a full-up MAJCOM, yet more than 67 percent of our work force are "traditional reservists" who for the most part, successfully balance a full-time civilian career with the part-time job of Air Force

professional.

You'll see that our mission is too broad to be categorized as just part of the combat air forces, mobility air forces, special operations forces, or Space Forces. AFRC folks do it all and are ready to fight in support of CAF, MAF, SOF and space.

The mission of AFRC is "to provide citizen airmen to defend the United States and protect its interests through aerospace power." Thus, we're the "force provider to the force providers." You'll see that in the comm and info business, that statement leads AFRC/SC to two simply-stated mission essential tasks:

- * Provide fully trained and equipped comm and info warriors to meet the needs of the AEF

- * Provide comm and info tools for the entire command's contribution to the AEF

The articles on the 349th and 514th Communications Squadrons' role in Operation Enduring

Freedom show how well we're doing that first task. A 100 percent Reserve crew from both units deployed to two Southwest Asia bases this year and ran the entire base comm mission. Both have since been deactivated and the squadron members are back to being teachers, firefighters, engineers, truckers ... ready to be called again when needed.

Task two gets done in many ways. There are 35 wings in AFRC, giving Lt. Gen. James E. Sherrard III, AFRC commander, an extraordinarily wide span of control. Thirteen of those

wings are based on AFRC-owned and operated bases, so we operate a

wide-ranging MAJCOM enterprise network (see AFRC Enterprise Network Re-IP, Page 10). The other 22 wings are tenants on active duty (and even a couple of ANG) bases, so co-

operation with all the other MAJCOMs is paramount for us.

At host wings, our comm and info troops do what comm squadrons do everywhere in the Air Force: take care of the base network, comm infrastructure, airfield systems, information management, etc. The difference is that we have no active duty personnel in these units. Everybody working during the week is an Air Force civilian, a contractor, or a special breed called an Air Reserve Technician, a uniform-wearing reservist who also happens to hold a civil service job tied to his/her Reserve position. Training time is limited for traditional reservists who train for their deployable mission at least one weekend a month, so the ART's job is to "prep the battlefield" for this training.

At tenant wings, the active duty host base comm squadron provides most base services, so the AFRC comm and info unit has a relatively small, but important, day-to-day comm and info presence, providing systems administration, information opera-



Col. Richard M. Jensen

“ ... we're the 'force provider to the force providers.' ”

tions/information assurance, information management, workgroup management and other services that help integrate the wing into the host network. Each tenant wing also has a deployable comm and info mission consisting of traditional reservists and equipment, so the ART's training job is no less important there.

At our MAJCOM headquarters at Robins AFB, Ga., we've got all the (sometimes unenviable) headquarters staff tasks that other MAJCOM SCs have. Here, though, is the one place in the command with an active duty presence. I'm an active duty, career comm and info officer, as is about one-third of my officer and enlisted staff. (Read that, "There's plenty of opportunity for everybody in AFRC!")

I'm proud to have the privilege to lead this diverse, professional bunch of comm and info warriors. Questions or comments? E-mail us at afrc.sc@afrc.af.mil.





AFRC plays integral role in daily AF mission

ROBINS AFB, Ga. – The Air Force Reserve Command, with headquarters at Robins AFB, became the ninth Air Force major command on Feb. 17, 1997. Prior to this, the Air Force Reserve was an Air Force field operating agency established on April 14, 1948.

Mission

AFRC plays an integral role in the day-to-day Air Force mission.

AFRC has 35 flying wings equipped with their own aircraft, and nine associate units that share aircraft with an active duty unit. Four space operations squadrons share a satellite control mission with the active force. More than 620 mission support units in AFRC are equipped and trained to provide a range of services, including medical and aeromedical evacuation, aerial port, civil engineer, security force, intelligence, communications, mobility support, logistics and transportation operations.

Organization

The Office of Air Force Reserve, in the Pentagon, is headed by the chief of Air Force Reserve, a Reserve lieutenant general, currently Lt. Gen. James E. Sherrard III, who is the principal advisor to the Air Force chief of staff for all Reserve matters. He is also commander of AFRC.

Headquarters AFRC supervises the unit training program, provides logistics support, reviews unit training, and ensures combat readiness. Within the headquarters element are all the normal MAJCOM staff functions, including directorates for operations, logistics, comptroller, communications and information, civil engineering and personnel.

The 4th Air Force at March ARB, Calif., 10th AF at Carswell ARS, Texas, and 22nd AF at Robins ARB, Ga., report to Headquarters AFRC. They act as operational headquarters for their subordinate units, providing training, operational, lo-



Photo by Bob Jacob

A C-130 from the Reserve's 910th Airlift Wing, Youngstown ARS, Ohio, performs an aerial spray mission.

gistical and safety support, and regional support for geographically separated units.

Air Reserve Personnel Center, a direct reporting unit in Denver, provides personnel services to all members of the AFRC and Air National Guard. Services include assignments, promotions, career counseling and development, and separation actions. ARPC also manages the individual mobilization augmentee program for the Ready Reserve, and maintains master personnel records for all Guard and Reserve members not on extended active duty.

Reservists are categorized by several criteria in either the Ready Reserve, Standby Reserve or Retired Reserve. Numbers below reflect assigned, rather than authorizations.

The Ready Reserve is made up of 193,000

trained reservists who may be recalled to active duty to augment active forces in time of war or national emergency. Of this number, 72,000 are members of the Selected Reserve who train regularly and are paid for their participation in unit or individual programs. These reservists are combat ready and can deploy anywhere in the world in 72 hours. Additionally, 49,000 are part of the Individual Ready Reserve. Members of the IRR continue to have a service obligation, but do not train and are not paid.



Lt. Gen. James E. Sherrard III

The president may recall Ready Reserve personnel from all Department of Defense components for up to 270 days. Some 24,000 Air Force reservists from 220 units were called to active duty during the Gulf War to work alongside active duty counterparts.

The Standby Reserve includes reservists whose civilian jobs are considered key to national defense, or who have temporary disability or personal hardship. Most standby reservists do not train and are not assigned to units. This category includes 17,000 reservists.

The Retired Reserve consists of 52,000 officers and enlisted personnel who receive pay after retiring from active duty or from the Reserve, or are reservists awaiting retirement pay at age 60.

Selected Reserve members train to active duty standards through the unit training or IMA training programs. Mission readiness is verified periodically, using active-force inspection criteria.

Reserve training often is scheduled to coincide with Air Force mission support needs. Since most AFRC skills are the same needed in peace or war, training often results in accomplishment of real-world mission requirements.

Unit Training Program

There are 60,188 reservists assigned to specific Reserve units. They are obligated to report for duty one weekend each month and two weeks of annual training a year. Most work many additional days. Reserve aircrews average more than 100 duty days a year, often flying to carry out national objectives.

Air Reserve Technicians work as civil service employees during the week in the same jobs they hold as reservists on drill weekends. ARTs provide day-to-day leadership, administrative and lo-

gistical support, and operational continuity for their units. More than 9,500 reservists, more than 15 percent of the force, are ARTs.

The AFRC's IMA training program is made up of about 13,000 Individual Mobilization Augmentees. They are assigned to active duty units in specific wartime positions and train on an individual basis. Their mission is to augment active duty manning by filling wartime surge requirements.

The AFRC Associate Program provides trained crews and maintenance personnel for active duty owned aircraft and space operations. This program pairs a Reserve unit with an active duty unit to share a single set of aircraft. It's a cost-effective way to meet increasing mission requirements.

Assigned Aircraft

AFRC has 447 aircraft assigned. The inventory includes the latest, most capable models of the F-16 Fighting Falcon, O/A-10 Thunderbolt II, C-5 Galaxy, C-141 Starlifter, C-130 Hercules, MC-130 Combat Talon I, HC-130 Tanker, WC-130 Weather, KC-135 Stratotanker, B-52 Stratofortress bomber and HH-60 Pave Hawk helicopter. On any given day, 99 percent of these aircraft are mission-ready and able to deploy within 72 hours. If mobilized, these aircraft and support personnel are gained by Air Combat Command, Air Mobility Command or Air Force Special Operations Command.

Real-World Missions

A proven and respected combat force, AFRC is quick to lend a helping hand. Humanitarian relief missions involve anything from repairing roads and schools in a village in Central America, to airlifting supplies into a war-torn city, to rescuing victims of nature's worst disasters.

At the request of local, state or federal agencies, AFRC conducts aerial spray missions using specially equipped C-130s. With the only fixed-wing capability in DOD, missions include spraying pesticides and compounds used to control oil spills. Other specially equipped C-130s check the spread of forest fires by dropping fire retardant chemicals. Real-world missions include weather reconnaissance, rescue, international missions in support of U.S. Southern Command, and aeromedical evacuation.

AFRC also takes an active role in the nation's counternarcotics effort.

(Information compiled from HQ AFRC/PA fact sheets)



AFRC comm and info

Just the facts...



Air Force Reserve Command has about 3,400 communications and information reservists authorized for units across the continental United States. Thirty-six CONUS communications units provide comm and info support to 13 AFRC bases, Air Reserve Personnel Center, three Reserve numbered air forces and 600 Reserve units worldwide. The communications units train to mobilize in 36 to 72 hours, and when activated, are gained by Air Combat Command, Air Mobility Command, Air Force Special Operations Command, Air Education and Training Command, and AFRC.

AFRC's Communications and Information directorate provides comm and info warriors and tools for Aerospace Expeditionary Force support and real-world contingencies.

AFRC/SC has four divisions that enable responsive and reliable communications and computer systems guidance, services and support. The readiness and combat support division (SCF) provides wartime and peacetime planning, functional oversight for manpower, and planning for deployable communications and AEF support. The operations division (SCO) provides command, control, communications and computer support to HQ AFRC functional directorates and field units, as well as operating the AFRC Network Operations and Security Center. The architecture and integration division (SCT) provides technical advice and assistance for the integration of communications-computer systems within AFRC by developing plans that detail communications-computer systems objectives and strategies. The plans, programs, and resources division (SCX) provides all planning, programming, budgeting, acquisition, and plans implementation for all communications-computer systems resources to the command.

Typical functions

Communications units are organized to provide both fixed and deployable support. Typical func-

tions are network support, information protection, e-mail, air traffic control and landing systems, Freedom of Information Act and Privacy Act programs, ground radios, and computer systems support. Reserve communications units may provide some or all of these functions. Unit capability is determined by assigned mission.

Host Base

Communications units provide day-to-day operational support to the 13 AFRC host bases and deployable support to gaining major commands.

Deployable

Deployable communications units provide additional comm and info support capability for real-world and exercise contingencies. Ten communications squadrons and 27 communications flights support deployable missions.

Two communications squadrons and three communications flights provide AMC initial communications packages for global reach laydown support. Global reach laydown provides a forward mobility infrastructure and reachback capability for worldwide airlift and tanker operations.

One combat camera squadron provides direct imagery capability in support of operational and planning requirements during worldwide crises, contingencies, exercises and wartime operations.

One communications squadron and five communications flights augment wing initial communications packages for ACC flying wings.

Two associated combat communications squadrons provide additional mission capability, with manpower and equipment for combat communications groups.

One communications squadron provides command and control for special operations forces.

Multi-Command

Comm and info personnel throughout AFRC provide postal support packages for AMC, U.S. Air Forces in Europe, and Pacific Air Forces. They also provide initial comm and info augmentation packages for active duty units.

(Information compiled from HQ AFRC/PA fact sheets, HQ AFRC, Robins AFB, Ga.)

Reorg postures comm and info for future missions

By Lt. Col. Margaret L. MacMackin
Air Force Reserve Command
Robins AFB, Ga.

In 1999, Col. Martha Maurer, then director of Communications and Information, Headquarters Air Force Reserve Command, asked the headquarters SC staff to review the Reserve communications and information function. The review analyzed functions, duties and responsibilities, as well as the comm and info organizational structure, mission, unit type codes, and all position descriptions. The assessment identified a need to restructure the comm and info function and organization at all levels, from the headquarters to the field units.

The transformation began in 2001 and proceeded in four phases. Phase one involved the headquarters comm and info staff, which was still aligned as it had been before the AF Reserve became a major command. It was realigned into four divisions with functions more in tune with today's comm and info mission.

More than 60 PDs were rewritten during this phase. This has better described the required duties and clarified staff roles. Phase one was completed last month.

"I arrived just as the reorganization was being implemented," said Col. Richard Jensen, the current HQ AFRC/SC, "and already I see the benefits of this transformation. There's a more clear division of work between MAJCOM responsibilities and support. This was clearly a gray area in the previous structure."

Phase two, which is nearly finished, saw an almost complete reorganization of the comm and info structure at the 13 AFRC host bases. The restructuring brought host communications squadrons and flights more in line with the active duty structure. It included a complete scrub of core functions and realignment of workload. The goal is to ensure the command's comm and info warriors are orga-

nized and trained to accomplish peacetime and wartime missions.

The command is in the early stages of phase three. The HQ AFRC SC and XP staffs completed a workload study at the 25 bases where AFRC units are tenants. The SC staff is collecting information on organizational structures, host/tenant support agreements, and civilian and Air Reserve Technician PDs. Based on the study, several Air Force Specialty Codes changed and the comm and info, personnel, and manpower communities are developing a clearer alignment of required duties and updating or writing new PDs that reflect the workload and match the newly identified division of labor and skills. This phase should be completed by the end of this year.

The fourth and final phase of the transformation will be to review the structure, duties and responsibilities, and PDs at the command's three numbered air forces at Dobbins AFB, Ga., Carswell ARB, Texas, and March ARB, Calif.

A final review will ensure all critical comm and info requirements have been identified. Change is inevitable in this career field, but in the end we'll be better postured for the future.



Photo by Staff Sgt. Ricky Bloom

Maj. Mike Lankford, a Reserve A-10 pilot from New Orleans NAS, La., climbs a ladder to the cockpit of his aircraft preparing to fly a close air support mission out of Afghanistan for Operation Enduring Freedom.



AFRC Enterprise Network

Efforts ensure network is ready and reliable

By Capt. Guy Cote
Air Force Reserve Command
Robins AFB, Ga.

Tell a Network Control Center they have to change their IP (Internet protocol) address range and you'll see a range of emotions from apprehension to excitement. Changing IP addresses, also known as re-IP, affects every user on the network since an IP address is a unique number that iden-

tifies a computer or printer on the network. Multiply that by 16. This is the task handed to the AFRC re-IP team, a small group of dedicated people with a big job: take a class B IP address range of 65,000 addresses, split it across 16 Reserve locations, and bring them behind the firewalls at HQ AFRC by the end of October 2002.

The team of six individuals from the AFRC Communications and Information directorate's operations division has the monumental task of traveling to 13 host bases and three other locations where we maintain the network:

- Re-IP the base network
- Remove the local firewall(s)
- Remove dial-up remote access service server
 - Consolidate Domain Name Server across the command to Windows 2000
 - Train and mentor personnel
 - Respond to emergencies

Working with the command network engineer, the re-IP team came up with a template to use at the bases. With manning assistance from the AFRC NOSC, the teams deploy on one-week visits.

The re-IP effort has roots in various areas: server consolidation, AFRC Common User Virtual Private Network deficiencies, and NOSC-centric capabilities.

Server consolidation is an Air Force downward-directed project, initiated as a result of the Air Force Information Technology Summit in July 2000. Server, desktop and network consolidation was directed as a means to right-size and right-place IT to reduce costs and free scarce manpower. AFRC server consolidation consists of series of projects distributed across two phases with a goal to physically consolidate all IT services to AFRC base NCCs and/or the AFRC Network Operations and Security Center at Robins AFB.

To meet DOD and AF requirements to encrypt sensitive information traveling on computers between the AF Enterprise, the AF Network Operations Center implemented the CU VPN. However, it does not





Howard Bedford, AFRC re-IP team member, and Tia Reed, AFRC NOSC, prepare connectors for an upcoming re-IP.

work across discontinuous subnets, and with more than half of the host Reserve locations using class C IP address ranges off “bigger” bases’ class B ranges, these locations were not able to use the CU VPN.

With the Air Force doing more with fewer people than ever imagined, the reliance on network availability to accomplish the mission will continue to grow. The AFRC Enterprise Network must be ready and reliable. This is where enhancements in NOSC-centric capabilities come in. New toolsets are being added to the NOSC that will give faster insight into the health and status of the AFRC Enterprise Network.

The re-IP effort will benefit all of these areas.

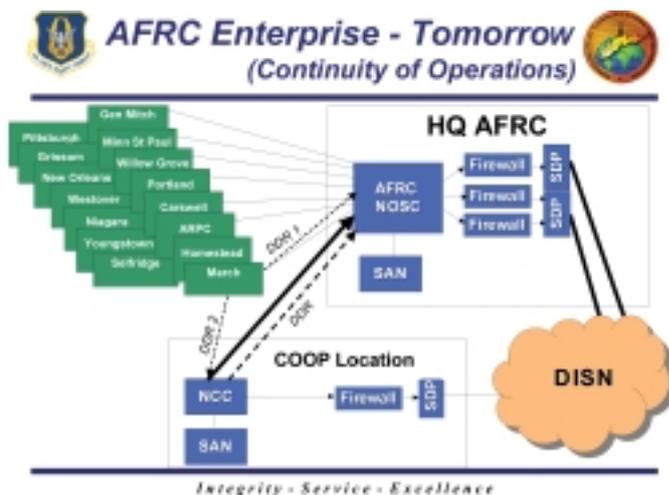
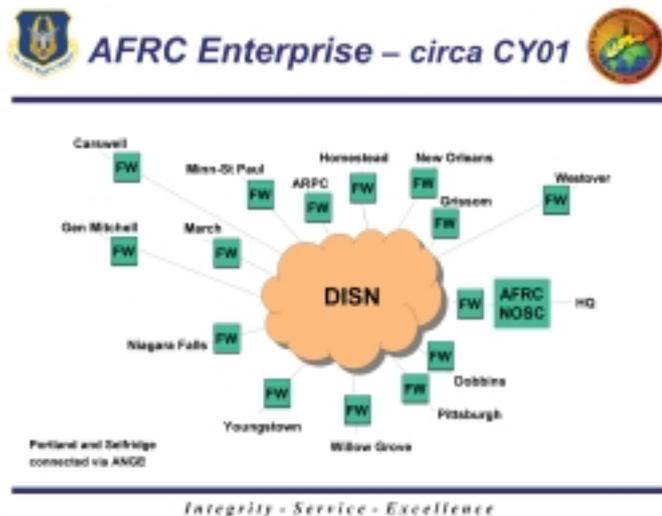
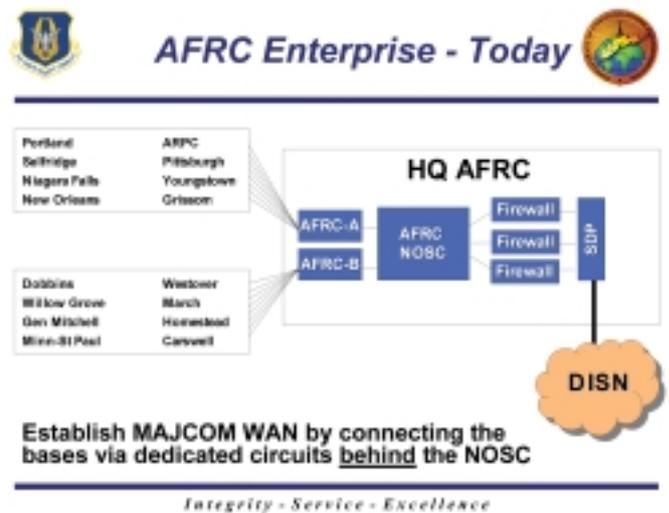
For server consolidation, the re-IP effort will result in removal of 64 servers across the command (remote access server, firewalls, external DNS, and Outlook Web access servers) and return manpower to the base NCCs.

As for the CU VPN, it is extended to Reserve locations through encryption modules in the “back-end” routers (AFRC-A and AFRC-B) which the 16 locations connect to at HQ AFRC.

The goal is to provide failover capability by establishing a continuity of operations location with dial-on-demand routing to the bases. If a disconnect is detected, the base router will call the COOP location to establish a path to NIPRNet until primary connection is restored.

Lastly, it will enhance NOSC capabilities: single enterprise firewall policy; standardized DNS at all bases to Windows 2000; improved RAS capability with 56kb service command-wide with single billing point; and 50 percent reduction in latency between AFRC locations across the enterprise network.

See NETWORK Page 12





NETWORK

From Page 11

Like every other MAJCOM, AFRC operates a MAJCOM enterprise network. Ours consists of 16 locations, each with an NCC (13 Reserve bases, two wings at ANG bases, and HQ ARPC) and a MAJCOM Network Operations and Security Center—the heart of the enterprise—is at Robins AFB. Network support for the additional 20 AFRC wings on active duty bases are supported like any other base tenant.

The enterprise re-IP effort began in February with a site survey at Willow Grove ARS, Pa., and the actual re-IP in March. From there, the team was split into two teams to finish the re-IP by last month. Augmented by personnel from the NOSC, the teams moved constantly throughout the states.

Rapid turnaround is the toughest part of the job. Re-IP team members usually must juggle two visits per month; a site survey at Base X and the re-IP for Base Y. During the site survey, they gather as much data about the base as possible. They then assign IP addresses, build the objects to be put in the firewalls back at headquarters so base-unique traffic will flow, and coordinate the information across multiple program offices and AFNOC.



Tech. Sgt. Lawrence Walker, AFRC re-IP team member, watches as Roy Dickerson, AFRC NOSC, provides training to Cariren Danson, AFRC NOSC, on how to load objects into AFRC's firewalls.

The road time the re-IP team members endure is taxing, but they feel a sense of accomplishment when the base has been re-IPd and things are running smoothly. They know there's no time to rest on their laurels. Even as this article is written, the same team members are preparing for the AFRC NOSC relocation.

Capt. Brian Jabes (left), a Reserve network engineer from AFRC Systems and Networks Flight, discusses router and switch configuration changes and provides training to Staff Sgt. James Wilmoth, AFRC NOSC, and Staff Sgt. Todd Keller, 939th CF, at the Portland IAP ANGB, Ore., NCC.



Strategic efforts move AFRC IT acquisitions from reactive to proactive

**By Capt. Robert C.
Kitchen**

*Air Force Reserve Command
Robins AFB, Ga.*



To achieve information superiority, the Air Force relies upon information technology as an enabler to collect and analyze intelligence, reduce decision cycle times, and plan campaigns. To gain this competency, the Air Force must acquire IT to maintain strength in today's complex and rapidly changing IT environment.

With shrinking budgets, new missions, more complex information systems, and greater reliance on IT, the Air Force can't afford to simply 'follow the market'. IT acquisitions are appropriately termed 'investments' as these expenditures are expected to give us strategic and tactical advantages over adversaries, both in the short- and long-term. It's imperative that those who acquire IT on behalf of the Air Force make their decisions *strategically* with an understanding of today's mix of limited resources and mission capabilities, as well as tomorrow's supportability and new mission requirements.

Ensuring that IT solutions are applied in the right places, at the right times, and in the right amounts across the Air Force can be challenging. Without the benefit of corporate vision, an asymmetric situation of 'haves' and 'have-nots' occurs based more on effective advocacy than on mission need. Even if funding wasn't an issue, an uncoordinated acquisition of IT across a large organization can lead to nonstandard/incompatible configurations and architectures, supportability problems, and limited flexibility.

Corporate visibility finds common solutions for common needs

To meet these challenges, in 1998 the Air Force Reserve Command initiated a command IT management program, which is now administered by the AFRC Chief Information Officer council, board, and working group. IT requirements are submitted by field units, through their numbered air forces, and go through the AFRC requirements process. AFRC then prescribes either a policy solution or a technical solution.

Technical solutions are included in the AFRC IT plan for fiscal year execution. This gives the added benefit of corporate visibility into where common solutions can be applied to common needs. It also limits the deployment of proprietary systems and allows for more efficient systems support. The AFRC CIO corporate body advocates for funding and tracks IT expenditures, which in turn alleviates this burden from the units. If local commanders still wish to keep the requirements process within their purview, the contract vehicles used for IT purchases at AFRC are available to the field. However, most AFRC units have taken advantage of the AFRC central IT plan, which has satisfied about 95 percent of fiscal year '02 AFRC IT requirements.

Each quarter throughout the fiscal year, the CIO working group, with representatives from HQ

See **STRATEGIC** Page 14



STRATEGIC

From Page 13

USAF/RE, AFRC headquarters, Air Reserve Personnel Center headquarters, and each of the three AFRC numbered air forces, corporately ensures IT requirements (hardware, software, infrastructure and technical support) are identified, prioritized and postured for execution once resources are approved and allocated. This satisfies the command's highest priorities and most other technical refreshment and sustainment needs.

Central to this plan is the submission and centralized collection of IT requirements along with a corporate IT acquisition strategy. The AFRC CIO board, consisting of headquarters staff directors, reviews the centralized IT requirements list to ensure it reflects AFRC mission needs. The AFRC CIO council, consisting of the major command and NAF/CCs, reviews and approves the centralized plan for execution. Using this approach, AFRC has already realized significant benefits since 1998, such as:

- ▶ More than \$11.5 million in savings over list prices by leveraging the power of conglomerate purchasing along with Air Force standard contracts
- ▶ Requirements are quickly identified, budgeted and supported
- ▶ IT is applied where needed; leveling the IT

playing field between 'haves' and 'have-nots'

- ▶ Enhanced configuration management and control through standardizing configuration of hardware and software across the command
- ▶ Incorporated support for MAJCOM functional downward-directed systems/new mission requirements
- ▶ AFRC CIO corporate structure oversight of IT/national security system investments

Since units may have immediate needs or requirements that can't be fulfilled through this process, AFRC has an alternate process that allows units to purchase IT that is consistent with the command's IT strategy and Air Force standards. AFRC maintains accountability of these local expenditures by establishing an IT IMPAC card specifically for the purchase of all software regardless of cost, all computer-related items that exceed \$500, and all Personal Digital Assistants. The unit can make these purchases at the same unit prices negotiated in AFRC's conglomerate purchase agreements.

The result: an IT acquisition plan that is lucid, unambiguous and effective. The insight that the command IT management program affords also enhances success in requesting additional funding during the financial planning cycle and budget drills. Overall, the coordinated efforts have moved AFRC IT acquisitions from reactive to proactive, paving the way to information superiority.

By Lt. Col. Margaret L. MacMackin

*Air Force Reserve Command
Robins AFB, Ga.*

Diverse staff keeps AFRC comm and info running at peak performance

The Headquarters Air Force Reserve Command communications and information staff has all the responsibilities of any major command staff, but the workforce is a little different. Col. Richard M. Jensen, HQ AFRC/SC and an active duty officer, oversees a headquarters staff of more than 170 people.

The staff is composed of active duty, Air Reserve Technicians, Air Guard reservists, civilians, and contractors. In addition to the full-

time staff, about 60 comm and info traditional reservists are assigned to the headquarters. This combination of personnel brings a distinctive blend of skills, knowledge, perspectives, and abilities.

"I thought I knew a lot about the Air Force after 27 years in the communications and information business, but the diversity of this workforce continues to amaze me and teach me new things," said Jensen. "In my assignments throughout the Air Force, this is unique. The staff here is one of the most professional, dedicated groups of individuals I have ever

Continued next page

Continued from previous page

encountered. Many positions are one-deep, but somehow our people get the job done, and done well. One of my challenges is that I have to be constantly aware of the diverse makeup of this staff.”

The AFRC staff faces many day-to-day challenges. In February 1997, the Air Force Reserve was redesignated as Air Force Reserve Command. This brought added responsibility to every directorate but no additional manpower. SC not only picked up additional responsibilities as a MAJCOM staff, but also faced the additional challenge of having to keep up with the explosion of information technology. In addition, AFRC comm and info units were selected for an A-76 cost comparison review in 1999. This process added a significant new workload for the staff.

Being a MAJCOM that resides on another MAJCOM-owned base brings another set of challenges. Our basic telecommunications support is provided in an outstanding fashion by the Air Force Materiel Command communications squadron assigned to Robins AFB, but the AFRC Network Operations Security Center maintains and supports the AFRC network. The local AFMC civilian personnel office classifies all AFRC civilian position descriptions.

Another unique characteristic is that AFRC/SC has a comm and info operations division (SCO). It is responsible for not only the day-to-day comm and info support to the headquarters staff, but provides operational support to Reserve wings, groups, and geographically separated units. It also runs the command-wide enterprise network, providing centralized oversight of the Reserve network systems. Similar to other MAJCOMS, AFRC/SC has a NOSC, but we also run a Network Control Center. Both the NOSC and the NCC are part of SCO.

These are just a few features that make AFRC



Photo by Staff Sgt. Shane Cuomo
A B-52 bomber takes off from a forward operating area on a combat mission in support of Operation Enduring Freedom.

different from the other eight MAJCOMs. Every day the AFRC staff deals with unique challenges, performing standard MAJCOM functions as well as day-to-day operational functions. This staff stands up to challenges and makes a difference.

“I’ve got a great job for a senior communications officer. In addition to headquarters work of policy, programming, budgeting, and managing the functional area, I’m never far away from the day-to-day hands-on of supporting this and our command-wide enterprise network. I’m proud to lead these pros.”



Server database keeps consolidation efforts on track

By Lisa Woodson
Air Force Reserve Command
Robins AFB, Ga.

“Server consolidation” is an Air Force-wide project, initiated as a result of the Air Force Information Technology Summit in July 2000, whereby server, desktop and network consolidation was directed to reduce costs and free scarce manpower.

Each major command is managing its own program within AF-defined architectural standards. AFRC server consolidation consists of a series of projects distributed across two phases with an end-goal to physically consolidate all IT services to either the AFRC Base Network Control Centers at each Reserve base and/or the AFRC Network Operations and Security Center at Robins AFB.

The cornerstone of the AFRC server consolidation effort is creating an enterprise mindset and approach. Successful enterprise planning required enterprise visibility, so one of the most challenging aspects of server consolidation within AFRC initially was how to obtain and maintain sufficient awareness of the type and number of servers currently fielded throughout the MAJCOM.

In a stroke of good timing, shortly before the AF server consolidation goals were announced in a SECAF memo, the AFRC headquarters architecture staff had just completed a survey of all network equipment, including servers, at each AFRC base. Although this data was only a static snapshot and could not fulfill the continuing need for progress tracking, it did provide the command-wide server inventory baseline needed for initial consolidation planning efforts.

To maintain current server status, the baseline data was folded into a relatively simple Access database, with a Web-enabled front end which allows designated base-level users the ability to update their server information as changes happen. More than just providing a box count, the AFRC server database provides information on the location, owner, technical specifications, function, and applications supported by each server in the command.

By providing HQ AFRC visibility and immediate access to complete and current information on

HQ AFRC Data for SERVER - #0011131284

[Back to the AFRC Server Database System Home Page](#)

Input your changes below and click the "Update Inputs" button to SAVE your changes!

MANUFACTURER DATA				
Site #	Machine Name	Manufacturer	Model	Status
0011131284	SERVER001	GATEWAY	E-5300	In Use

LOCATION DATA				
Parent Office	POC Name	DSN	Relig	Room
EOG	Analyst One	485-1744	E10	25
In NCC?	Admin'd by NCC	NIPR/SIPR		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

COMPONENT SPECIFICATIONS				
Processor Spd (MHz)	# of Proc	Processor Type	RAM (MB)	Oper SYS
100	1	486	512	NT Server
Total HD Space (GB)	Free HD Space (GB)	RAID 5	NIC Card	
0	0	<input type="checkbox"/>	10/100	

Server Roles

Please indicate the role(s) of this server - (Mark all boxes that apply)

<input type="checkbox"/> HP OpenView	<input type="checkbox"/> RAS	Domain Controller: <input checked="" type="checkbox"/> Primary <input type="checkbox"/> Backup
<input type="checkbox"/> TTS/Assembly	<input type="checkbox"/> ASIM	Firewall: <input type="checkbox"/> In Use <input type="checkbox"/> Not Standby
<input type="checkbox"/> BDEMS/SQL Server	<input type="checkbox"/> Proxy	DNS/DB: <input type="checkbox"/> Internal <input type="checkbox"/> External
<input type="checkbox"/> Non-DMS Email	<input type="checkbox"/> DHCP	<input type="checkbox"/> Primary <input type="checkbox"/> Secondary
<input type="checkbox"/> DNS	<input type="checkbox"/> SMS	WINS: <input type="checkbox"/> Primary <input type="checkbox"/> Secondary
<input type="checkbox"/> NMS		WEB: <input type="checkbox"/> Internal <input type="checkbox"/> External
<input type="checkbox"/> FTP	<input type="checkbox"/> CBT	
<input checked="" type="checkbox"/> File	<input type="checkbox"/> CD	
<input type="checkbox"/> Printer	<input type="checkbox"/> Tape Backup	

OTHER ROLES: In this server running DNS:

Parental Office: Application Name: Description:

For multiple Applications, list in COMMENTS block below

COMMENTS
<input type="text"/>

all servers throughout the command, the AFRC server database enables server consolidation planners to quickly and consistently respond to a variety of progress and compliance reporting requests, without burdening the field with continuous data calls. The AFRC server database also provides data to calculate projected savings and return on investment for the command's consolidation effort.

Beyond server consolidation reporting, the AFRC server database is an enabling technology as it supports enterprise-wide server configuration management and the AFRC centrally managed IT plan, as well as ensures accurate server counts for server operating system licensing and upgrades.

AFRC expected to have all AFRC core servers (e-mail, file, print, Web, network management) consolidated at either the NCC or NOSC by publication time. Consolidation of all functional servers will be completed within the year, or so, in accordance with Air Force-wide memorandums of agreement.

Comm and info reservists support war on terrorism

By Capt. Jay Custine
Air Force Reserve Command
Robins AFB, Ga.

The men and women of the Air Force Reserve Command who work in communications and information have always played a major role in our nation's involvement around the world and at home. In daily support of the Air Force mission, comm and info reservists could be found at work on every continent, responding on short notice, ex-

actly as advertised. Intended to provide wartime augmentation, the units and personnel also provide daily comm support of national objectives, serving whenever the need arises.

The world changed after Sept. 11, 2001, and Reserve comm and info support changed with it. Demands for all types of communications increased drastically and the qualified individuals to provide and manage this support became high demand.

Comm and info professionals of the AFRC have provided extensive support to the war on terrorism. The contingency requirements filled by Reserve comm and info personnel increased 600 percent over the Aerospace Expeditionary Forces support levels before Sept. 11. These contingency requirements covered a range of comm and info duties at several deployed locations.

Thirty-nine volunteer reservists deployed to air defense sector headquarters to support Operation Noble Eagle. Many agreed to stay for extended rotations. The duties they performed spanned comm and info specialties, including administrative, electronics maintenance, and watch officer for the crisis action team.

Reserve comm and info personnel also supported several Operation Enduring Freedom rotations, including Global Hawk and Theater Deployable Communications - Integrated Communications Access Package. Volunteers from the 911th Communications Squadron at Pittsburgh Air Reserve Station were deployed for extended rotations to support the initial deployment of the Global Hawk program.

One of our most significant comm and info contributions has been the deployment of personnel from the 514th CS at McGuire AFB and the 349th CS at Travis AFB. Members of these squadrons were deployed to two OEF sites to provide the full range of TDC-ICAP support services, including secure and nonsecure voice, video, and data. These squadrons collectively provide half of the AMC total force capability for TDC-ICAP support.

The Air Force Reserve will continue to play a vital role in the total force for all future contingencies, and the comm and info professionals will always answer the call.



Photo by Master Sgt. John Nimmo

Tech. Sgt. Sai Yu, an Air Force Reserve computer network and crypto switching systems specialist, 514th CS, McGuire AFB, N.J., tests for dial tone on newly installed phone lines at a forward deployed location in support of Operation Enduring Freedom.



McGuire reservists spring into action

By **Capt. William Davies**
514th CS
McGuire AFB, N.J.

Their motto is "When the day comes," and it was never more clear than in the wake of Sept. 11 attacks.

People at the 514th Communications Squadron, McGuire AFB, knew that as one of Air Force Reserve Command's Theater Deployable Communications units, the day had come and they were ready to support wartime operations in the Operation Enduring Freedom area of responsibility. Two 90-day rotations had to be supported by two 18-person global reach bed-down teams. This marked the first time the 514th CS was ever activated in its 20-year history.

The 514th CS relieved personnel from their associated unit, the 621st Air Mobility Operations Squadron Communications Flight. The mission for the 514th was to sustain 24/7 communications and install new voice and data services. The 514th was tasked to operate and maintain the Network Control Center, base telephone network, ground radio maintenance facility, COMSEC custodian function, and systems control center. The 514th also handled all automated data processing equipment requests as well as the base public address system.

The transition to the TDC mission began in 1999, before the unit was even tasked to its new role. The first part of the plan was to co-locate the



Photo by Master Sgt. John Nimmo

Senior Airman Lawrence Mangino, an Air Force Reserve computer network and crypto switching systems specialist, 514th CS, fills in the new phone numbers on a junction box to lines he has just installed at a forward deployed location in support of Operation Enduring Freedom.

514th CS Air Reserve Technicians with Air Mobility Command's active duty 621st AMOS CF. This integration was a win/

win situation for both organizations. It resolved a constant active duty problem of personnel turnover by ensuring qualified trainers were available. This also ensured the reservists had full access to equipment and facilities needed to become mission capable.

The second part of the plan was to conduct joint training in which both organizations did a lot of benchmarking and information sharing. Not only were the reservists prepared to meet the needs of this technical mission, they were requested by the 621st AMOS commander to relieve his active duty team.

The first team, made up of traditional reservists, and led by Capt. William Davies, left in March and returned in June. During their deployment, they overcame multiple issues and learned what it meant to support more than 200 telephone users and 800 network users.

The team had only three days transition time with the departing 621st AMOS team. Even so,

they hit the ground running and took charge of the C4I systems at the base. Their first challenge was to reestablish the Secure Internet Protocol Network, or SIPRNet. They coordinated fix actions at various bases in the AOR and with NOSC-D at Shaw AFB. Contributing to the immediate restoration of the service was the Cisco router and network management expertise that Tech. Sgts. Todd McAllister, Peter Proscia, Tammy Kisamore, and Mark Collings brought from their civilian backgrounds. Besides manning the NCC, the customer support team of Tech Sgt. Tanya Brandon and Senior Airman Melissa Mefferd immediately helped all users.

Information assurance and security was the task of the COMSEC CRO, Tech. Sgt. Patrick Generoso. His efforts yielded zero security incidents and ensured all computer viruses were identified, quarantined and eradicated with zero downtime to data networks.

Another issue was how the base VHF air-ground radios were configured. The noncommissioned officer in charge of the ground radio section, Tech. Sgt. John Reyes, made sure the command post and war operations center had 100 percent connectivity with all aircraft. This section was also tasked to install the base Giant Voice system, critical in alerting the base populace of attacks and threats.

The telephone switch team protected and repaired base wire infrastructure. Tech Sgt. Charles Smyler led the team of Tech. Sgt. Pat Guarragi, Staff Sgt. Chris Burress, Senior Airmen Errol Senior and Vincent Majors, and Airman First Class Anthony Ciletti to develop a long-term plan that

ensured all fiber optic cable would be protected from the intense heat and sunlight, as well as vehicle and foot traffic. The task was completed in one week and it protected more than 50 miles of fiber optic and CAT-5 cables.

The team also had to reconfigure the entire phone switching system due to a failing module. They accomplished in six hours what would have normally taken two days while eliminating outages that averaged 20 hours a week.

The first team's preparation for redeployment paid off with the arrival of the second team led by Maj. Andrew Abraham and Master Sgt. Israel Rosado. The subject matter experts from the second team had been in constant communication with the first team so they were able to hit the ground running.

Although their mission was the same as the first team, the excessive heat was a challenge. The temperature climbed over 110 degrees by 9 a.m. The team did most repairs at night but urgent requirements made daytime repairs a necessity. Besides the weather, the second team was tasked with optimizing the base wiring infrastructure. The team developed a plan to remove all unused wires and evaluate the physical condition of operational circuits. This task was completed in three days and enabled the team to quickly identify wires of failing circuits.

The second team's NCC crew, led by Master Sgt. Edward Williams, was tasked to activate a SIPRNet circuit using TACLANES. This modern encryption device will replace Motorola NESs in future iterations of the TDC package.

Both teams were integrated with communications personnel from the Washington State Air National Guard. Their mission was to support the ground mobile force satellite terminal and provide the management element for the 384th Expeditionary Comm Flight.

The 384th ECF commander best summed up the dedication and commitment of the 514th CS. Maj. Craig Kowald thanked the leadership of the 514th CS for providing the 384th ECF highly trained, professional and motivated communicators. "Their efforts played a vital role in the mission of the 384th AEG and have shown that the Air Force Reserve is a key part of the total force. I would go to war with these people anytime, any place."



Tech. Sgt. Alvaro Bonilla and Senior Airman Dylan Imperato align a PSC-5 antenna on top of the 384th Air Expeditionary Group's war operations center.



'Tactical' is our middle name

Squadron sends TDC package to provide initial comm at OEF site

By Maj. K. Bosko
349th CS
Travis AFB, Calif.

The 349th Communications Squadron, an Air Force Reserve tactical communications squadron at Travis AFB, has built a reputation throughout the Air Force Reserve and the active duty communications arena. If you have a tactical communications job, they are ready to do it. They were recognized as the 2001 Communication and Information Organization of the Year for AFRC.

During the last week of September 2001, the 349th CS sent two members to forward locations when an active duty unit needed to fill shortfalls. Master Sgt. John Yingst and Staff Sgt. Che Lau were notified and on a plane within 15 hours, providing ground radio support for two locations.

"Organized chaos at a very small site with no communications equipment" is how Yingst described his first impression of the deployed location. Not only was the communications team building base infrastructure, they were also base security for the site, and cooks for the base chow hall, earning the title "jack of all trades".

Just after installation of initial communication, all communications equipment had to be redeployed to another location. This involved the complete removal of all cable and equipment so it could be used at the new location. During their 100+ day deployment, the team completely built-up two sites

and assisted on a third.

In December, when Air Mobility Command determined its next location to build a transportation hub, an active duty communications squadron was tasked with providing the equipment and personnel. Due to other commitments, the squadron could provide most of the equipment but none of the personnel. This gave the 349th CS an opportunity and a challenge. Its A-team accepted the assignment. Active duty equipment was quickly and thoroughly operations-checked, palletized, and prepared for shipment. The squadron then selected

22 highly trained individuals from a core 60-person squadron. This would be the squadron's first wartime deployment with the Theater Deployable Communications Integrated Communications Access Package.

After a few long flights, the team arrived at its bare base in Southwest Asia. With no communications infrastructure, the job started at square one. Arriving at

sunrise, the team never unpacked and instead went straight to work. A flying base needed communications and they were the ones to do it.

Some members of the team didn't fully unpack their personal gear for weeks. With no engineering and installation support available, the small team became experts at digging through coral rock by hand, wearing out three pick-axes in the process. With the tally still growing, the 349th CS has installed more than 7,000 feet of fiber optic cabling, 107,000 feet of copper cabling, 3,000 feet



Staff Sgt. Jonathan D. Grace, 349th CS, digs through coral rock to lay conduit for a fiber run.

Continued next page

From previous page

of conduit, terminated 50 pairs of fiber, installed 500 Ethernet and 300 DSN drops. They supported a base populace of up to 1,200 users, 250 Non-Secure Internet Protocol Router Network computers, 50 Secure Internet Protocol Router Network computers, and 150 DSN phone lines.

Seven unique solutions were created for Army proprietary systems, and five emergency base telephone networks with priority access for vital communications needs. Six thousand requests for service were handled. They provided communications for two major operations and the day-to-day missions supporting the warfighters in Afghanistan and Pakistan.

Their customer base was primarily a combat support battalion and an aerospace expeditionary group. From the troops' perspective, the biggest achievements were wiring the tent with audiovisual for the projection TV for Superbowl XXXVI

and providing e-mail capability to communicate with families. "The Army appreciated each and every thing we did for them; they were incredible customers," said Maj. Craig Wells, 349th CS commander and deployed team chief.

After 134 days in the sand, the A-team was replaced by the B-team. Seamless to the customers, from project conception through implementation, here was teamwork at its best. The Long Reach Ethernet implementation project involved both teams enabling extension of NIPRNet services to previously isolated user enclaves. This project involved a partnership with Cisco Systems and the A-team to obtain the equipment, and the B-team installing and implementing the services.

Although still in the buildup phase of deployment, the second team was also moving toward the sustainment phase. Relocating the TropoSpheric Satellite Relay system and the Giant Voice installation were two major projects accomplished by the second team.

Regional CAW manages DMS registration, fortezza cards for 16 AFRC locations

By Lt. Col. Sidney O. Wade
*Air Force Reserve Command
Robins AFB, Ga.*

Air Force Reserve Command established a regional Certificate Authority Workstation facility to manage the Air Force Defense Message System registration process for organizational messaging and to produce DMS fortezza cards for 13 AFRC bases and three other locations where we maintain the network and the command headquarters.

Staffed by five full-time employees, the facility became operational in June '02, and will produce both unclassified and classified cards. The regional CAW consolidates the workload of the current five AFRC base-level CAWs, eliminating this workload from base-level communications units. It dramatically reduces training costs and provides an easier transition for future certificate upgrades.

AFRC is the first MAJCOM to stand up a regional CAW. The process of

regionalization is fraught with problems when information on the status of each and every fortezza request (X.509 certificate request form) is not known to both base-level and regional CAW personnel, so AFRC developed a Web site for units to use when requesting cards.

Imagine a Web site where the customer can request and track order progress in a way similar to tracking an express mail package. Delivery times have improved dramatically, with an average time of less than seven days from receipt of the request to delivery of the card to the customer.

Emergency orders get overnight delivery. The new facility, linked via the 509 Web site to the customer base, puts AFRC in a position for success as the community prepares to field version 3 certificates.





4TH Combat Camera Sq plays key role in Millennium Challenge

Tech. Sgt. Keith Baxter, 4th CTCS, operates the weapon systems video/non-linear editor during Millennium Challenge 2002.

By 1st Lt. Hamilton Underwood
4th Combat Camera Squadron
March ARB, Calif.

Millennium Challenge 2002 deployed more than 40,000 U.S. troops and employed such cutting edge technologies as the tilt-rotor CV-22 Osprey, and the Army's Stryker medium armored vehicle. However, there weren't any fond farewells for these troops because all of them and their weapon systems were deployed only in the virtual world of megabits and gigabytes. The entire war scenario was simulated. It did, however, involve 13,500 personnel at nine separate training sites in the continental United States. The "deployed" troops were generated by 51 simulators as part of the U.S. Joint Services Command's testing of information technology tools over a two-year period.

At Air Force Plant 42 in Palmdale, Calif., the 4th Combat Camera Squadron from March ARB participated in the Weapons Systems Video/Non-Linear Editor portion of the exercise. Tech. Sgt. Keith Baxter was tasked as the WSV/NLE operator. His mission was to retrieve video imagery from pod-mounted cameras after combat aircraft returned from their sorties.

This imagery was then digitized on a non-linear editing system, which is designed to take analog 8mm video and convert it into electronic form for editing purposes. From this stream of imagery, individual clips of targets or battle damage were selected and burned to a CD-ROM. This imagery was then up-channeled via the SIPRNet to a central server so authorized users and theater commanders could view target selection and battle damage.

David B. Tressler, integration analyst for



Photo by Tech. Sgt. Sam Ameen

Weapons Systems Video (HQ USAF/ILCXD) said, "WSV allows theater commanders to see video within hours instead of days, allowing for timely and operational decision-making and strike analysis. It was only a few years ago that the process of retrieving video and presenting it for viewing could take several days. During Millennium Challenge 2002, the process from engine shutdown to the time the video was available on the central server was about an hour and a half to two hours. Tressler said, "That's a huge improvement from Gulf War technology."

For the 4th CTCS, the WSV is a brand new Unit Tasking Code. Millennium Challenge 2002 marks the first time this UTC has been deployed. "4th CTCS support was invaluable," said Tressler. "During the first two flights, they were the only WSV system deployed to cover the Global Strike portion of the exercise."

"This is a very important mission for the squadron," said Baxter. "It's rewarding to know

Continued next page

From previous page

that the imagery we up-channel goes to the theater level to help identify targets, assess damage, and will ultimately be an influence in future battles.”

The 4th CTCS director of operations, Maj. Tytus Harley, agreed, “It’s important that we deploy with other units involved in WSV. It helps us work out problems and ensures the processes we have in place work should we deploy in support of a real-world operation.”

Although many different airframes participated in the “live fly” portion of the exercise, the 4th CTCS worked directly with the imagery acquired from the F-117 Nighthawk under the command of the 410th Flight Test Squadron in Palmdale.

“This is a perfect example of technology, still in the developmental phase, being successfully implemented in a real-world test,” said Michael Seelos, project manager of F-117 participation in Millennium Challenge ’02, “Everyone here is incredibly pleased with the way the system has performed. The process of getting this video up the chain has been cut to minutes instead of days thanks to this near-real time system.”

While no one knows what the future of warfare may look like, Millennium Challenge puts a face to the many technologies the U.S. military will likely implement in the coming decade. For the 4th CTCS there is no question that Weapons System Video will play an important decision-making role for war planners as IT and security spearhead our entry into this volatile new millennium.

AFRC stands up 2 combat comm units

By Lt. Col. Margaret L. MacMackin

*Air Force Reserve Command
Robins AFB, Ga.*

In coordination with Air Combat Command, the Air Force Reserve Command stood up two Reserve combat communications units “partnered” with two active duty combat communications units.

On Oct. 1, 2001, the 55th and 35th Combat Communications Squadrons were activated. The 55th CBCS “partnered” with the 5th Combat Communications Group, Robins AFB, and the 35th CBCS “partnered” with the 3rd CCG, Tinker AFB, Okla.

The AF Reserve previously had three stand-alone combat communications flights: the 94th CBCF at Dobbins ARB, Ga., the 911th

CBCF at Pittsburgh IAP ARS, Pa., and the 914th CBCF at Niagara Falls IAP ARS, N.Y. Not only was the mission of these units scheduled to terminate in fiscal year ’04, their equipment was aging and transitioning to new systems would be costly.

On Oct. 1, 2001, the 94th CBCF was inactivated and the 914th and 911th CBCF were inactivated June 1, 2002. To maintain the combat communications capability, in early 2000, the HQ AFRC directorate of Communications and Information began working with the combat/base systems division, HQ ACC/SCC, to find a new mission for these units.

While ACC and U.S. Air Forces in Europe combat

See **COMBAT COMM**
Page 24



Master Sgt. Ray Kurle holds the 55th CTCS guidon prior to the assumption of command ceremony.



COMBAT COMM

From Page 23

communication units were transitioning to Theater Deployable Communications packages, ACC still had a requirement to retain Tri-Service Tactical (TRI-TAC) communications equipment the U.S. Army and Marines continue to use.

The two commands decided to stand up two Reserve communications squadrons partnered with two active duty combat communications units to support the TRI-TAC requirement and eventually transition to the TDC mission. The Reserve squadrons would first be the AF TRI-TAC bridge capability, filling the void left as active duty combat comm units transitioned to TDC. They then would transition to TDC packages to support that mission with the active duty.

This decision allows the Reserve to transition to a needed mission and have access to not only TRI-TAC but TDC equipment as well. The active duty gets trained, experienced combat comm troops to augment their requirements and the ability to retain knowledge and expertise on TRI-TAC equipment while they move to TDC. As the Reserve squadrons transition to TDC equipment, the active duty will have a cadre of trained, experienced reservists who can train active duty troops as they rotate in and out of the 3rd and 5th CCGs.

The two units activated Oct. 1, 2001. The 55th



Maj. Pete Peterson, (right) accepts command of the 35th CBCS from Col. Mario Goico, 507th Air Refueling Wing vice commander.



Representatives from each of the 5th Combat Comm Groups' mission squadrons await the start of the ceremony.

CBCS consists of two 64-person Theater Air Base UTC packages, while the 35th CBCS consists of one 64-person Theater Air Base UTC package. Eventually, ACC will transfer the equipment suite to support the TRI-TAC capability to the 35th and 55th CBCSs. Each unit brings personnel to organizations stretched thin by ongoing deployments and contingencies, while obtaining training on the more advanced tactical communications equipment.

Both units will be able to use equipment, training resources, and share facilities with the active duty units to enhance their capabilities and give them a viable tactical communications mission. As each unit becomes operationally capable, they also bring additional resources to the respective groups. Most importantly, once they are fully capable, they bring a cadre of highly motivated and trained combat communicators to augment the ongoing deployments the groups support and provide assistance during contingencies.

Reservists tend to stay in one area longer than the active duty personnel, so they become a repository of corporate knowledge. The result is the Reserve becomes the mission and training continuity for both the TRI-TAC equipment and eventually TDC. As the 35th and 55th CBCSs become fully capable, they too should provide continuity to the 3rd and 5th CCGs.

This is a tremendous opportunity for the reserve and the active duty as these two units partner to support the deployable communications community--total force at its best.

New system makes tracking supplies easier

By Petty Officer Gary Henry

Navy Information Bureau Kansas City
Scott AFB, Ill.

In Afghanistan and other austere locations, U.S. troops are now able to better track their orders of vital supplies. That's because of efforts by U.S. Transportation Command officials to improve the "in-transit visibility" of people and cargo moving through the Defense Transportation System.

"Tracking makes planning easier," said Lori Jones, chief of the in-transit visibility branch at USTRANSCOM. Unfortunately, that has not always been the case, she said. The whereabouts or in-transit visibility of people and cargo is frequently a mystery to the frontline warfighters who need that information the most, she said.

In-transit visibility is the military's long-sought goal to clearly track the identity, status and location of traveling people and cargo from origin to destination, and to make that information available to warfighters throughout the chain of command.

That means now, with a few clicks of a mouse on a laptop in Afghanistan, a supply sergeant can tell his commander that a crucial shipment of parts from the United States has landed in Kabul and is scheduled to arrive by truck the next day.

"ITV is crucial for planning, in war or peace," Jones said. It is more of a reality now, she said, at close to 100 percent manifest level reliability for intratheater. But until recently, it was a dream, particularly in

and around Afghanistan.

The need for a reliable tracking system became painfully apparent during Operations Desert Shield and Desert Storm. Thousands of containers arriving in theater had to be opened and inspected just to find out what was in them before sending them on, Jones explained. It cost time, effort and uncertainty.

As recently as December, Operation Enduring Freedom troops in U.S. Central Command had difficulty tracking their re-supply items such as food, water and ammunition they needed to get the job done.

"These locations are remote and austere," Jones said. "There's no infrastructure. Units were filling out logistical paperwork, but it wasn't going anywhere into any kind of reporting system.

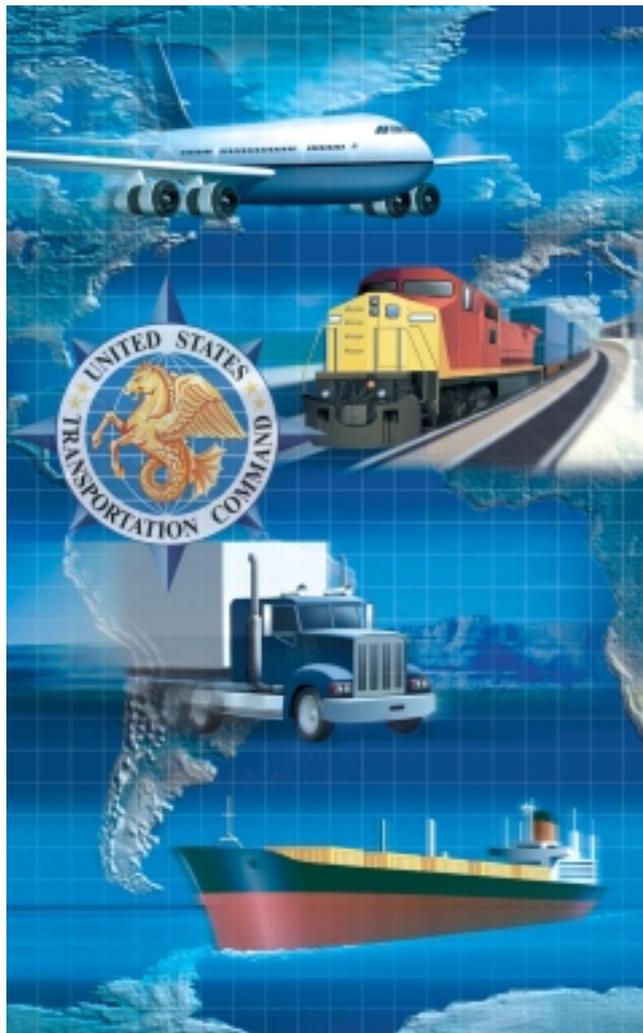
People just couldn't tell where and when the things they needed would arrive."

The effort to support the warfighter and provide near-real time ITV began in earnest right after the terrorist attacks of Sept 11, Jones said.

That is when USTRANSCOM's Brig. Gen. Gil Hawk headed up a "cell" or task force whose job was to resolve differences in tracking and reporting procedures throughout the different branches.

"They resolved firewall and data exchange issues throughout all the different services," Jones said. "The team consisted of active-duty military, reservists, government civil-

See TRACKING Page 26



Joint STARS testing takes off at Edwards

By Rob Bardua

AF Flight Test Center Public Affairs
Edwards AFB, Calif.

The Air Force's Joint Surveillance Target Attack Radar System aircraft, Joint STARS, is becoming a familiar site on the runway here.

The aircraft and its test team from Melbourne, Fla., are participating in the Defense Advanced Re-

search Projects Agency's Affordable Moving Surface Target Engagement, or AMSTE program, developed by Northrop Grumman.

The program is demonstrating the ability to precisely engage moving surface targets with modified precision-guided weapons. The Joint STARS, an airborne battle management and command and control system, is proving key to the AMSTE test program.

In ongoing testing, real-time information on a moving target is developed from radar sensors. The resulting tracking data is relayed from a Joint STARS aircraft directly to a modified weapon sys-

See **JOINT STARS** Page 29

TRACKING

From Page 25

ians, and contractors. They worked 24/7."

By December, Hawk's group laid the groundwork for ensuring critical information exchanges were clearly passed to USTRANSCOM's Global Transportation Network. GTN links the services and defense agencies logistics systems throughout the DOD and the commercial carrier information into one integrated database. GTN is the DOD's designated in-transit visibility system of record.

That done, the effort took on an operational flavor and focused energy to ensure CENTCOM locations had needed capability to report movements into and out of the theater, Jones said. Air Force Maj. Gen. William Welser III led the cell in putting reporting and tracking procedures in place for logisticians throughout the military — with an emphasis on getting people in the remote and dangerous areas of USCENTCOM plugged into the system.

Air Mobility Command, part of USTRANSCOM and also based here, sent special training teams into Afghanistan. The teams installed equipment and trained aerial port workers on how to use the latest technology.

Jones explained that within weeks the teams brought the ability to receipt and process critical movements into and within the theater supporting Operation Enduring Freedom.

Though that was a priority, Welser's group continued — and continues today — to train logisticians across the DOD, in order to get everyone more fully plugged in to GTN.

Discipline and compliance with documentation procedures is the key. As with any automated system, garbage in equals garbage out, said Jones. Training is vital so that personnel understand the key role they play ensuring senior leaders and troops across the board have the necessary information for decision-making.

"So we're constantly training, tracking and refining the system," she said.

"We've had several days in a row of 100 percent ITV," Jones reports. "On Aug. 22, we had the cargo and passengers reported on 53 of 53 intratheater missions, and on 21 of 23 intertheater missions (97 percent ITV). This is just a portion of the total spectrum."

"We never expected this level of success so soon," Jones said. "Back in January we were hoping for a 60 percent ITV rate by summer."

Though USTRANSCOM and DOD officials have made logistical improvement in ITV, they are still only about a third of the way to where they want to go.

"Total asset visibility is our ultimate goal," Jones said. She explained that while GTN can report on items in transit, material in storage or in repair is a different story. Discussions and research are under way on TAV. *(Courtesy of USTRANSCOM News Service)*

Airborne surveillance system keeps security forces safe

By Rhonda Siciliano

*Electronic Systems Center Public Affairs
Hanscom AFB, Mass.*

Deployed security forces supporting Operation Enduring Freedom can now see beyond base perimeters and visually assess detected threats quicker thanks to the latest in unmanned aerial vehicle technology.

The Electronic Systems Center's force protection system program office experts delivered the initial Force Protection Airborne Surveillance System that "adds an enhanced layer of protection for bases around the world," said Col. Howard Borst, program office director.

Each system consists of a ground control station, which has a computer, displays, recorder and communications equipment; six UAVs; a remote imagery viewing terminal; interchangeable payloads of color cameras and thermal imagers for day and night imagery; and transportation cases and launch equipment. The UAV flies primarily at 300- to 500-feet and gives operators real-time overhead video data.

"One of its strengths is the ease with which it can be reprogrammed in flight," said Maj. John



Photo by Staff Sgt. William Greer

Airman 1st Class Michael Burns, from the 438th Expeditionary Force Protection Squadron, prepares to launch an airborne surveillance aircraft at a forward-deployed location supporting Operation Enduring Freedom. The aircraft provides the base with another layer of defense without putting lives at risk by transmitting live footage to the operator as it surveys the perimeter of the base.

Crennan, delay denial systems division chief.

A two-man crew operates the system. Operators launch the UAV using a bungee cord catapult. Flight missions can be pre-programmed, and with the touch of a button on a laptop computer, altered to monitor an area.

"The system is not intended to be 'backpackable,' but it's easily transported by a general purpose vehicle," said Crennan. The UAV, dubbed "Desert Hawk" by Lt. Gen. T. Michael Moseley, 9th AF and U.S. Central Command Air Forces commander, is small, lightweight and very simple to operate, Crennan said. The airframe is manufactured from damage-resistant molded material designed for limited field repair. Desert Hawk can operate from a 100- by 100-meter clearing without a runway.

"FPASS was designed to be used by cops," said Maj. Mike Giger, FPASS program manager. "It extends the range security forces can monitor without putting troops in harm's way."

"This system is not intended to replace troops," said Borst. "It's a critical surveillance tool that will protect and save lives by providing essential real-time information on potential threats." Air Force experts from the FPASS program met with members of the Marine Corps UAV program office to discuss opportunities for collaboration. The Marines are developing their own UAV system known as Dragon Eye.

The FPASS system is designed to operate close to a base, while the Marine Corps requires a more rugged system that can operate under a variety of harsh environments, he said.

"There's a great potential for collaboration on our UAV programs that we already know of," said Bruce. "If we can collaborate on subsystems and tailor less expensive items to meet our individual needs, then we'll be marrying jointness of the systems while allowing for individual needs of each service," said Bruce.

The Air Force and Marine Corps have signed a memorandum of agreement to share information on UAV development.

"We're already looking for opportunities to enhance interoperability as we progress - which will result in cost savings," said Borst.

(Courtesy AFPN and AF Materiel Command)

'Enterprise architecture'

By Tech. Sgt. Scott Elliott
Air Force Print News
Washington

Transformation, the Air Force chief of staff said, is the key to the service's future.

To that end, Gen. John P. Jumper said the service needs to stop concentrating on individual systems. Rather, the Air Force's air, space and ground platforms must work together by sharing information to accomplish the mission.

"Enterprise architecture" is the Air Force's blueprint process to bring together its individual systems to form this integrated capability. Just as an architect designs a building to ensure all its parts work together and make sense, enterprise architecture will use models and processes to capture the complex interrelationships between the Air Force's many systems and platforms.

It also will ensure that this integrated view is linked to the Air Force's requirements, planning, programming and budgeting, as well as its acquisition processes.

"Enterprise architecture lets us effectively deal with the enormous complexity of integrating the large number of different components that contribute to performing Air Force missions," said John Gilligan, Air Force chief information officer.

Essentially, he said, the goal of the Air Force's architecture efforts is to point the way to the future for the Air Force in terms of innovation, and, more importantly, in terms of simplicity.

"The goal of Air Force enterprise architecture is to provide the roadmap for innovation and to function as a blueprint for improving the overall leverage of valuable information technology resources," Gilligan said.



Blueprint process brings together individual systems to form integrated capability

"Gen. John Jumper is very articulate in the explanation of his goal for the Air Force," he said. Jumper's goal, dubbed "horizontal integration," refers to that sharing of information among various systems and platforms.

"You need all of the air, ground and space elements to interact to achieve the synergy envisioned by (General Jumper)," Gilligan said. "However, the complexity of this starts to exceed our ability to deal with it in the human brain, or to write in text, (so) architecting, using formal methods and tools, then becomes the answer."

The true value of enterprise architecture becomes apparent as leaders look to future budgets. According to Gilligan, the architecture will allow people to determine if something should be funded in a particular year's budget based on how the capability contributes to mission accomplishment.

Perhaps more importantly, the architecture could prevent the accidental misspending of money on related items.

"If we can't fund (a project) this year, there may be no sense in funding another project, because we need both to provide the desired operational effect," he said. "In the past, we did not process analytical tools to help identify these issues."

Another benefit from enterprise architecture is the capture of the required system-to-system interactions, which then becomes requirements to

See ENTERPRISE next page

JOINT STARS

From Page 26

tem in flight, such as Boeing's Joint Direct Attack Munition, or JDAM, or Raytheon's Joint Stand-off Weapon, or JSOW.

"We're finding a way to attack moving targets on the ground with affordable, smart (global positioning satellite-type) weapons," said Col. Bob Hood, director of the Joint STARS test force in Melbourne, Fla., in charge of testing for the Joint STARS E-8C aircraft. The test force's overall mission is to develop surveillance and battle management capabilities for all services.

After taking off from Edwards during recent test flights, the AMSTE team engaged in complex moving target scenarios at the Naval Weapons Center in China Lake, Calif. These flight experiments demonstrated multiple, simultaneous JDAM weapon deliveries and integrated AMSTE technologies with the JSOW.

According to Hood, first the Joint STARS aircraft must establish a communications link with another radar system, in this case Northrop

Grumman Electronic System's BAC-1-11 test radar. Together, the two radar systems track a moving vehicle along the ground while "talking" to the weapon, he added.

Finally, the data link guides the weapon in flight onto the vehicle moving on the ground.

"The Joint STARS aircraft provides a comprehensive look at the moving targets on the ground," said Hood. "As we move into the MC-2A airplanes that we're developing for the future, we're going to be fusing more information from more sensors and drastically reducing the time from sensor to shooter."

The MC-2A is a modified Boeing 767 containing a multimission command and control aircraft system. Hood's team is looking at incorporating information from Global Hawk and other unmanned aerial vehicles and adding sensors to provide an integrated air and ground picture.

"By doing so, we'll be able to more quickly find, fix, track and target those elusive moving targets that are so important to prosecuting a fast and furious war," Hood said. "We will be able to deny one of the last sanctuaries to our enemies."



E-8C Joint STARS aircraft

ENTERPRISE

From previous page

be satisfied in the acquisition process.

"The systems architecture should define how the F/A-22 Raptor interacts with an airborne warning and control system aircraft, (which is) interacting with an air operations center," Gilligan said. "This system architecture then feeds into the requirements process for individual systems as well as the budget and development processes."

In the past, Gilligan said, three separate documents had to be generated to achieve the same result.

"We'd write a requirements document, an acquisition document and a budget document, and they would all be different, for different purposes," he said. "Now, as we go forward using architectures, we'll have the relationships defined, and the (same) requirements description in the form of architecture products can be used for the budget jus-

tification and by the acquisition community."

Because the enterprise architecture system is so vast, various agencies have been identified to manage certain areas. For example, Gilligan said Air Force Space Command will manage architecture activities for space-related missions, and the deputy chief of staff for installations and logistics will be responsible for logistical architectural needs.

While the term "enterprise" represents the Air Force in its entirety, Gilligan noted that the enterprise architecture concept does not stop there.

"Air Force architectures have to fit a broader context," he said. "We have a lot of efforts under way with the other services and the joint community...so we're going to make sure our architecture approach is in harmony and we can use our architectures to better understand how air and space capabilities can support joint and coalition efforts as well."

FY '03 Scope Eagle class dates set

Scope Eagle is a “seminar” type course conducted at Keesler AFB, Miss. Attendees are selected to attend by a nomination/selection process.

The nominations are collected/consolidated by Air Force Communications Agency/XPIC and the selections are made by Air Force/ILCX.

The course provides senior executives in the communications and information systems and related career areas a forum to refresh themselves technically, discuss policy issues of corporate concern and prepare to lead in a future marked by rapid technological change.

Attendees will receive updates on current Air Staff policies and issues. Participants have the opportunity to broaden individual perspectives by discussing problems, issues, and solutions with key leaders, managers and peers in the career areas

as well as selected industry representatives.

Because the curriculum changes to reflect current issues, all colonels and GM/GS-15s should plan to attend every three to five years to keep abreast of the changing technological environment.

Prerequisites for the course are:

Attendance is restricted to colonels and GM/GS-15s in the 33XX career areas or related specialties.

Lieutenant colonels and GM-GS-14s in selected positions may also attend.

The class dates for fiscal year 2003 are:

Feb. 3-7

March 17-21

June 9-13

July 21-25

Sept. 15-19



Information protection: *Know user responsibilities*

By Brig. Gen. Richard E. Webber
*AFSPC Director of Communications
and Information Systems
Peterson AFB, Colo.*

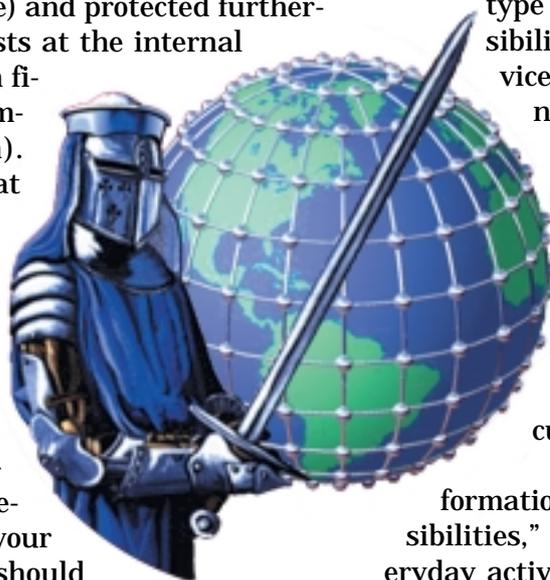
As the new SC at AFSPC, I want every one to know how important I believe your duties are for the protection of our information. In today's information technology age, nearly all our information runs across the world through networking technologies. Protecting the Air Force's network is much like protecting a base itself. On a base you have a fence, gates, doors to buildings, doors to the offices within, and the people at different levels protecting them throughout. Similarly, within a network there exists a network boundary (fence) protected by a firewall to get in (the gate) and protected furthermore by access control lists at the internal routers (buildings), which finally terminates at the computer itself (the room). Again, you have people at different levels responsible for protecting each of these areas.

As a user, your responsibility is to protect not only your information, but the entire base's information as well. Specifically, the first line of defense our network has is your password. Each of you should be well aware of the Air Force's standards in creating a difficult password, but do you know why? Some users have the attitude that their password doesn't matter and there is nothing of value on their specific system. What they don't realize is that their password not only grants access to their system but to the network as well. Any compromised password can allow the malicious hacker to gain initial access, which in time, can be elevated. According to the AFSPC Network Operations and Security Center, there are millions of unknown and

potentially suspicious hits on our network every month. These hits represent a multitude of activities, to include state-sponsored intelligence gathering, a 14-year-old trying to make a name for himself, or plain and simple mistakes. Just this year one of our own bases was scanned by the Air Force Information Warfare Center's 92nd Information Warfare Aggressor Squadron and the results were frightening. After scanning several thousands of network devices, a quarter of them (all NT/2000 workstations) were hacked simply through the fact they had no passwords. This issue has been resolved but it was unsettling to know that the time leading up to these scans proved we were susceptible to a major network attack.

As many people are now taking advantage of these great "gee whiz" Personal Digital Assistant type products on the market, our responsibilities increase in protecting these devices when we use them for official business. We are also moving to one of the latest technologies, DoD Public Key Infrastructure, where our own ID card has become even more valuable to those trying to gain access to our base and our information. The point is, not only do we need to protect our information over our networks, but physical security is our responsibility as well.

As we recognize and promote the Information Assurance theme of "user responsibilities," I ask you to take a look at your everyday activities with the information you control. Do you own a PDA and if so, does it contain official information? Are you taking advantage of your common access control ID card on your office workstation? Is your password one that no one can guess easily? Do you scan your e-mail for malicious attachments? Do you scrutinize anyone's need to know when you are questioned about specific critical information? These are all things to think about, as you proceed in your daily duties, no matter what month it is. Know your responsibilities and live up to them.



User responsibilities: Why worry about computer security?

By Master Sgt. Keith Korzeniowski
and Jack Worthy

45th Communications Squadron
Patrick AFB, Fla.

Before going to bed at night, do you leave your front door unlocked? When parking your car, do you leave the keys in the ignition? Probably not.

You automatically take precautions to secure valuables. Information is a valuable asset for our national security. In the computer age, information has become the lifeblood of many companies.

Failure to safeguard information as you would your home or other assets is ludicrous. Unfortunately, according to a 1999 study done by the University of California all too often security measures are either minimized or ignored by 26 percent of the entire information technology and automated information system communities.

For those in the know, the need for computer security measures is apparent. Even though data assets can be lost, damaged or destroyed by various causes, information systems tend to be susceptible for several reasons.

Computer components are relatively fragile. Hardware can be damaged more easily than, for example, tools in an auto repair shop. Data files are extremely fragile compared to other organizational assets. Second, computer systems are targets for disgruntled employees, protestors and even criminals. Finally, decentralization of facilities and use of distributed processing have increased vulnerability of information and computers.

There are many ways to protect and prevent access to computer systems – from physical security involving locks and guards, to measures embedded in the system itself. Since end users have access, each represents a potential vulnerability. Many security measures begin with you.

Here are some guidelines:

- * Know your unit information systems security officer, and information assurance awareness manager, and phone numbers for the network control center's C4 help desk.

- * Assure your system is certified and accredited. Systems designated to handle classified in-

formation must complete an emission security assessment before processing is authorized.

- * Practice good password creation and protection. Assure passwords contain at least eight characters, including upper and lower case alpha, numeric and special characters, and are exclusive to your system.

- * Use a password-protected screensaver when leaving your computer unattended.

- * Share information only with people and systems authorized to receive it.

- * Always scan disks, e-mail attachments and downloaded files using the latest antiviral product and signature file.

- * Know the sensitivity level of the information you're processing, requirements for protecting it, and security limitations of systems used to transmit it. Sanitize processing and storage devices.

- * Know the basics of data contamination, malicious logic, and virus prevention and detection.

- * Avoid virus hoaxes and chain letters.

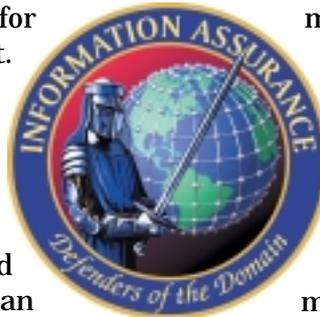
The telecommunications monitoring and assessment program governs consent to monitoring. Notification of consent is approved through signed permission and is placed on DOD computers, personal digital assistants, local area networks, external modems, phones, fax machines, text pagers, phone directories, and land mobile radios.

Being a base network user is like being a member of the local community, which provides services to its citizens. Just as a community has laws, the network has policies.

First, e-mail is for official use only. Policy is addressed in AFI 33-119, Electronic Mail Management and Use. Forbidden activities include sending or receiving e-mail for commercial or personal financial gain, and sending harassing, intimidating, or offensive material to or about others.

Like e-mail, Internet or Web access provided by the network is for official use only. AFI 33-129, Transmission of Information via the Internet, provides guidance on proper use of the Internet. Do

See **USER** next page



Password protection key to information security

By Master Sgt. James M. Howard
90th Communications Squadron
F. E. Warren AFB, Wyo.

Vulnerability, according to Webster's dictionary, means susceptible to attack. In relation to Air Force information systems, our goal is to identify and eliminate all vulnerabilities. The longer they go undetected, the greater the chance of an attack.

Everyone in the Air Force, in one way or another, relies on protection of sensitive information in automated information systems. Information attacks can severely hamper or even halt daily operations. Consider how effective you would be if your system were down for a day or even a week. Your job as a user is to prevent system vulnerabilities through password protection.

As a user, you're the one authorized to access the information system. You've completed required training, in some instances passed the background check, and have been deemed trustworthy to access the information system and all of its data. It's now your responsibility to safeguard the system by preventing access by unauthorized users.

How do you do that? By following one of the most basic fundamentals—proper password protection. When you were granted access to the system, you were given a user identification and you had to supply a password. Your user ID is generally known to those around you, but your password is not. You had to comply with several require-

ments for your password and you couldn't make it a simple dictionary word—for good reason. Dictionary words are part of the hacker's host of software tools for cracking your password. Your password unlocks the door to a database which, if manipulated or destroyed, could devastate operational capability and adversely affect information systems across the Air Force. It's your responsibility to prevent someone else from using it.

To ensure you're effectively protecting your password, here are some guidelines from AFMAN 33-223, Identification and Authentication:

- * Use passwords with at least eight alphanumeric characters (upper and lower case) with at least one special character (@, &, +, etc.).

- * Never make a password related to your personal identity, history or environment.

- * Change passwords every 90 days.

- * Memorize your password. Don't place passwords on desks, walls or sides of terminals, or store them in a function key, login script or communications software.

- * Don't share your password.

- * Establish a six-month minimum password age on the system to prevent anyone using former passwords.

- * Limit the number of attempts allowed for correct password entry. When the maximum is exceeded, lock out the user-ID or terminal.

Password protection is a key element in assuring network and information security.

USER

From previous page

not transmit offensive language or materials, such as hate literature and sexually harassing items, and obscene language or material, including pornography and other sexually explicit items. The AFI also prohibits obtaining, installing, copying, storing or using software in violation of the vendor's license agreement. Before downloading software from the Internet, keep in mind much of the freeware or shareware is only free for personal use. Licenses for many

programs exclude use by the government or commercial companies.

If you break the law in your community you can face serious consequences. What may be less known is that violating network policies also has consequences. A captain at Wright Patterson AFB was sentenced to nine months' confinement, a \$10,000 fine and a reprimand for conduct unbecoming an officer for using an Air Force computer to download and store pornographic images.

The base network is an un-

classified system and a shared resource. One careless user sending a classified e-mail over the network can mean the loss of e-mail and shared drive access for hundreds of users until the system is cleared. As a member of the base network community, be a good citizen.

Learn more about your role by completing the information assurance Internet-based training courses INFOCON and Licensing Network Users. For more information, see <http://214.3.105.136/default.asp>.

Philippides faced network threats in 490 B.C.

By Robert G. Rosack

Chief, Information Assurance
and Senior Computer Network Defense Analyst
Air Force Space Command
Peterson AFB, Colo.

In 490 B.C., Persian forces completed an amphibious assault upon the plain of Marathon near Athens. According to legend, the Athenians sent a runner named Philippides, or “Phil” for short, to Sparta requesting aid. Phil completed the 150-mile run in less than two days. Against overwhelming odds, the Athenian forces, led by Miltiades, defeated the vastly superior Persian army, led by Darius the Great, before Sparta could render aid.

Phil’s run was not in vain, because it serves as an example of one of the earliest documented military communications networks, composed of a sender (Miltiades), a message (“Help us”) and a receiver (Sparta). Phil himself constituted the media that conveyed the message. Today’s military communications networks face the same threats that imperiled the “Philippides Network.”

The five tenets of information assurance—availability, integrity, authenticity, confidentiality and non-repudiation—mitigate threats to information and information systems. We can imagine that Philippides used the same tenets to protect his message to the Spartans.

Availability is the most crucial tenant of information assurance. Philippides faced many perils. There was the distinct possibility that a faster Persian would catch him and perforate him with a spear, constituting a direct threat to availability of the Athenian message. Today, network availability is so important that by eliminating it, an adversary can negate the remaining four tenets.

Integrity involves protecting information from manipulation during transmission. Consider the message “Help us.” Had the Persians captured Phil and changed his message to “Don’t help us”, the consequences could have been catastrophic to the Athenian cause. Message integrity is vital to ensure our decision-makers have accurate and reliable information and networks.

Authenticity ensures parties to an information exchange are who they say they are. When Phil arrived in Sparta, how did the Spartans know

who he was? He likely presented himself as an authentic Athenian, which could be detected from his dialect and appearance. Perhaps he had an authentication certificate from Miltiades. Generally, we use the same authentication methods. We recognize specific characteristics, such as logon ID and password, to authenticate ourselves to a network. We’re also beginning to use electronic certificates and biometrics, including retinal scanners.

Confidentiality keeps the message private between the sender and receiver. If Phil hadn’t kept the nature of his message private, the Persians could have used the information against the Athenians. Today we rely on encryption to keep messages private. Historically our focus has been on classified information, but we’ve made increasing use of commercial-grade encryption technology (such as secure socket layers) to prevent casual interception of unclassified messages.

Non-repudiation ensures the sender of a message cannot deny sending it. How would Phil prevent Miltiades from denying that the Athenian general sent Phil to Sparta in the first place? Perhaps witnesses wrote of the event in diaries, creating a certification of the transaction between Phil and Miltiades. We use electronic certificates and signatures to witness the transactions made on our networks to ensure non-repudiation.

Modern networks are threatened in ways Philippides could not have imagined. He would not understand malicious code, such as viruses and worms, distributed denial of service attacks, or spoofing of Internet protocol addresses. He would understand the basic tenets of information assurance to protect information and information systems. To be of use, information must be available. He would understand the need to maintain integrity of information on our networks. Authenticity of information was as important to Phil as it is to us. He would understand the use of ciphers to keep information confidential, and the need for non-repudiation in information transactions.

Long before Philippides’ run, military communications has relied on the five information assurance tenets to protect military information. They will continue to be of paramount importance to sensitive communications in the 21st century.

Social engineering: Hackers exploit human weaknesses

By **Laurie G. Knepper**

Senior Computer Systems Manager

Joint STARS Test Force

Melbourne, Fla.

Do you understand the potential impacts of social engineering on the Air Force and national security? And the big question: Are you an unwitting participant?

Social engineering is a term used to define computer and physical security cracking techniques that rely on weakness in human nature rather than hardware, software or network design weaknesses. The goal of social engineering is to trick people into revealing passwords, revealing information about a computer system or network to expose security vulnerabilities, or revealing other information that will prove useful in obtaining unauthorized access to important data. Using social engineering, even someone with lousy computer skills can find their way into a supposedly secure computer system and access, modify or destroy the data on it.

How are your social engineering defenses?

* Do you lock your work station before leaving your desk—or do you leave it up to a screensaver to kick in a little while later?

* Would you decline to give your password to someone over the phone or in an e-mail who said they were debugging a problem with your account, and then contact your computer security representatives immediately—or would you comply with the password request?

* Do you challenge strangers in the hall who don't display a proper badge—or do you assume because they're in a nice suit that they are probably too important to be questioned?

* Would you stop a clean-cut uniformed deliv-

ery person carrying packages who flashes a smile and asks where the mailroom is as he attempts to "tailgate" into a secure building with you—or would you politely hold the door open for him and point him toward the mailroom?

* Do you shred old phone lists—or do you simply dump them in the trash or recycle bin?

* Would you decline to participate in a phone survey that asks a bunch of questions about your organization's computer systems—or would you participate to get the "free gift?"

* Do you leave work discussions at work—or do you discuss Air Force business over meals at local restaurants?

In case you have any doubt, the first action in each of the previous bullets reflects proper security practices, while the second action reflects poor security practices to outright security violations.

Here are a few interesting and educational links that deal with social engineering. Please read them. There may be a test. It may be given by someone official. Or it may be given by someone who's not official, not authorized, and not supposed to be getting the information or access that you're either willingly or inadvertently giving them. Think about it.

Physical Security - Technical Security's Biggest Hole lists some everyday "easy access" methods that have proven effective:

Physical Security - Technical Security's Biggest Hole lists some everyday "easy access" methods that have proven effective:

http://www.scmagazine.com/scmagazine/2001_11/feature.html

Social Engineering Fundamentals, Part I: Hacker Tactics:

<http://online.securityfocus.com/infocus/1527>

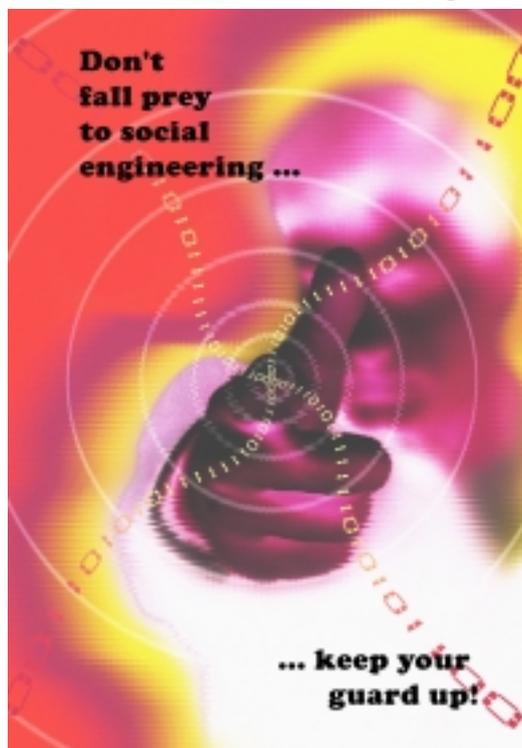
Social Engineering Fundamentals, Part II: Combat Strategies:

<http://online.securityfocus.com/infocus/1533>

Social Engineering Attacks via IRC and Instant Messaging:

http://www.cert.org/incident_notes/IN-2002-03.html

For more info, e-mail Laurie.Knepper@js-jtf.af.mil, or call DSN 854-5245, ext. 7103, or (321) 726-7103



Celebration of communications heritage

AACS alumni meet in Dayton



Lt. Gen. Harry Raduege, his wife Julee, and Chuck "Bogie" Bogovich



Dick Frye, retired Chief Master Sgt. Jeremiah Hayes, and retired Maj. Gen. Gerald Prather



A reunion attendee, Julee Raduege, and retired Lt. Gen. John L. "Jack" Woodward Jr.



Lt. Gen. Harry Raduege and Col. David Kovach

DAYTON — Dayton, Ohio, a city rich in aviation history, was all abuzz with communications history Sept. 26-29. Hundreds of retired communicators gathered there for a stroll down memory lane at the 26th annual AACS Alumni Association Reunion.

Richard "Dick" Frye, executive director of the AACS Alumni Association, welcomed guests and kicked off activities that looked at how aviation has shaped communications. This year people came from far and wide to renew friendships, relive memorable experiences from military assignments, and most importantly, to continue a deep family bond that grows stronger with time.

Much has changed since most of the attendees saw active duty, but one thing that hasn't changed is the camaraderie. The active duty communications community has a special relationship with the association and many active duty folks joined this year's activities.

The Association was created in 1977. It now has well over 2,700 members and continues to grow. The original association was comprised of individuals who served in the Army Airways Communications System and/or the Airways and Air Communications Service. In 1995 a proposal expanded the association to include individuals who served in AF Communications Service and AF Communications Command.

This year the association voted to extend eligibility to people who served or are serving in AF Command, Control, Communications and Computer Agency, AF Communications Agency, and AF Flight Standards Agency.

In addition to sharing war stories and reminiscing about communications experiences, the agenda at this year's reunion, hosted by Stan

and Jo Ann Phillips, included something for everyone: dinner theater, Air Force Museum tour, local attractions, and banquet.

Honorees include retired Colonel Bob Brewer, retired Master Sgt. Joe Duffy, and Tom Snyder, all selected as the first inductees into the AACS Alumni Association Hall of Honor. The Hall of Honor recognizes members for distinguishing themselves in the Air Force, civilian life, or in their communities.

The association also honored retired Colonel Bernard "Barney" Glettler and retired CMSgt. Hank Sauer with the AACS Life Achievement Award for exceptional service to the Alumni Association. The award honors members who have distinguished themselves in service to the association by devoting many hours, days and years to making the association one of the best.

Brewer, a long-time alumni member and past executive director, was honored just one year ago with the award of the Bronze Star Medal and Purple Heart for his heroic actions during the attack and sinking of the HMT Rohna 59 years ago. Brewer, then a lieutenant in the U.S. Army Air Corps, assisted others onboard after an attack by German bombers carrying rocket-powered guided missiles. Brewer helped other sailors and soldiers to the safest routes to abandon ship. He then spent eight hours in the water before being rescued. Brewer said he loved his days in AACS and AFCS, having served with communications pioneers such as Brig. Gen. Ivan Farman, Maj. Gens. Francis Ankenbrandt, Daniel Doubleday and Dudley Hale, and Lt. Gen. Harold Grant. (See story on Pages 38-39)

Duffy served in the military from 1955 to 1976 and was then em-

played as a civilian by U.S. Space Command, Falcon Air Station, Colo., as a satellite resources/satellite scheduler. Seeking more challenges, he joined the Department of State as a foreign services communications officer. Assignments included the American Embassy, Moscow; the American Embassy, Beijing; and the U.S. Mission, Berlin. He was later selected for duty in the State Department, Washington, D.C. From the time he entered the Air Force until retirement with more than 40 years of government service, his dedication and spirit for hard work has impressed peers and continues today.

Snyder is the historian for the AF Communications Agency, Scott AFB, Ill. He advises the AFCA commander and staff on all historical matters and aspects of the C4 community's history program. Under his direction, the AFCA historians research, write histories, and maintain an extensive collection of documents and photographs. His office serves as the corporate memory of the C4 community. Snyder and his staff pride themselves in providing the historical record and perspective for Air Force communications professionals to know the past, understand the present and anticipate the future.

Glettler was cited for his performance as treasurer, custodian of memorabilia sales, and as a board of directors member. He is recognized for establishing a set of ethical standards for all to follow. His skills in dealing with the entire membership provide a model for everyone in the association.

Sauer was recognized for his outstanding services as executive director for four years and for his service as the association's newsletter editor and publisher. In 2001, he became the first enlisted member of the AF Communications and Information Hall of Fame. "Hank's dedicated, unselfish and devoted service to our association is a shining ex-

ample of total commitment to one's comrades, organization and nation," said Frye.

Guest speakers during the banquet were Brig. Gen. Mike Peterson, 81st Training Wing commander, and Colonel David Kovach, AFCA commander. Retired Maj. Gen. Gerald Prather led a tribute to POWs/MIAs.

Peterson gave an update on Keesler AFB and on the state of the C4 community. He also emphasized how much he enjoys the reunions. "It's so much fun," he said, "sitting here, learning and remembering."

Kovach said he was proud to be in an environment where people are so proud of their service and each other. "I'm grateful to the men and women in this audience who laid the groundwork," he said.

Among the guests were Lt. Gen. and Mrs. Harry Raduege, director, Defense Information Systems Agency; retired Lt. Gen. and Mrs. John "Jack" Woodward, former Air Force deputy chief of staff for Communications and Information; Brig. Gen. Richard E. Webber, deputy chief of staff for Communications and Information Systems, Air Force Space Command; and former AFCC senior enlisted advisors retired CMSgts. Jeremiah Hayes and Ron Allison. Also attending the banquet were Colonel Andy Anderson, commander of the 88th Communications Group at Wright-Patterson AFB, and several enlisted personnel and spouses from the 88th CG. The Wright-Patterson Color Guard added an extra touch of class to the banquet.

Sauer said they told the young airmen to look around the ballroom to the more than 350 people and try to imagine themselves 50 years from now, running the AACS Alumni Association.

Next year's reunion will be held at Falls Church, Va. For more information or to join, check out the Web site: www.aacsalumni.com.



Dick Frye and Bob Brewer



Dick Frye and Tom Snyder



Dick Frye and Joe Duffy



Barney Glettler and Dick Frye



Dick Frye and Hank Sauer



Brig. Gen. Mike Peterson

Nov. 26, 1943

Communicator survived maritime disaster



Hundreds died when the German missile struck, the majority from exposure and drowning when darkness and rough seas limited rescue efforts.

Few have heard about the Rohna sinking—a tragedy that ranks with the greatest loss of American military lives at sea during wartime. Fifty-nine years ago, Nov. 26, 1943, the HMT (Her Majesty’s Transport) Rohna, a British transport ship carrying American soldiers, was hit by a German-guided bomb and sank off the coast of North Africa. More than 1,000 American troops were lost.

To keep the Germans from learning how devastating the attack was, the U.S. government kept the incident a secret. The event was lost to history for decades until survivors began sharing their memories with historians and reporters.

The memories still haunt survivors. One of those is retired Col. Robert M. Brewer. At the time of the Rohna attack, he was one of eight communications officers (lieutenants) destined for the China-Burma-India theater to become commanders of Army Airways Communications System units.

Of 135 AACS enlisted personnel on the Rohna, 75 were lost in the disaster. The men were special-

ists in air traffic control, navigation aids, radio operation and cryptographic devices.

Brewer was 26 years old and had been on active duty since 1939, reaching the grade of technical sergeant. He became a second lieutenant in April 1943.

The ship, packed with almost 2,000, was part of a convoy bringing troops to Burma when 35 enemy aircraft attacked, keeping up the attack for more than two hours. Several of the Heinkel 177 long-range bombers carried two remote-controlled glider bombs, one under each wing. The Hs293 was, in effect, the first air-launched cruise missile. A rocket engine launched the bomb away from the bomber; then it glided toward its target under remote (radio) control.

“There was very little warning over the ship’s alarm system,” said Brewer. “I was two decks below the boat deck with several other officers in our cabin. All personnel were immediately ordered to remain below the boat deck. We were able to see the attack through portholes on the port side one deck above our cabin.

“We saw the guided missile coming toward our ship,” said Brewer. “It struck the ship at midpoint above the waterline on the port side below our vantage point. It exploded upon impact and the concussion blew us into a hallway some distance away. The area became dark, with steam and fire nearby. We crawled toward the bow and climbed a stairway to the boat deck.”

“On deck we saw panic and devastation everywhere. Many men were injured, some dismembered, many needed attention. Hundreds were already in the water. We all



Art by George Wright, courtesy of Naval Historical Center.

had inflatable Navy type waist belts that helped save many," he said.

"We assisted as many of the injured as we could. The ship was on fire, listing and sinking. It sank in less than an hour. We lost 1,015 of some 2,050 U.S. (military) personnel aboard." The sinking also claimed three Red Cross workers and 134 Indian crewmen and British officers, making it the worst at-sea disaster in U.S. history.

"One has unknown courage and strength at a time like that and heroism was evident everywhere onboard and in the water," he said. Brewer sustained injuries when leaving the ship requiring hospitalization for several weeks. He was awarded the Purple Heart and Bronze Star Medal just a year ago in Stockton, Calif., by Congressman Richard Pombo.

Brewer said he was lucky to survive. He spent eight hours in the water before being rescued by a British tugboat—the HMS Mindful. "There were many heroes that night," he said. "With hundreds in the water there was panic in rough seas. Many were injured and many died in the water. The USS Pioneer, an escort minesweeper, rescued 606 men that night, many saved by the valiant efforts of the Pioneer's crew. To date we have been unable to obtain a national award for the bravery of that crew," said Brewer. The survivors have appealed to the Navy and Army for a citation.

After several weeks in a British hospital in Bougie, Algeria, Brewer joined other survivors in the Bizerte area at a replacement camp. They all were rescheduled to continue to the CBI theater for two to three years of duty. "I continued in AACS field commands at several locations in China and India. Back in the states, I was assigned to Headquarters AACS, Andrews AFB, and later at Headquarters AFCS, Scott AFB. I stayed with the command for nearly 27 years in all before my retirement in 1966."

Brewer and other survivors mounted a crusade to remember the Rohna. Brewer helped establish the Rohna Survivors Memorial Association several years ago and has served as its president since then. It has 500 members, including nearly 100 survivors still living and next of kin family members of those



Congressman Richard Pombo, right, presents the Purple Heart to Robert Brewer. Inset: Lt. Robert M. Brewer, age 26.

lost. They meet each year in May for a reunion, attracting about 300 each time. "We lived to tell the public that it happened. Our purpose is to continue to tell our unique story and to find others who might have been involved." Their Web site is at: <http://www.whidbey.net/rohna/rohna.htm>

Brewer said the Rohna tragedy ranks with the greatest loss of American military lives at sea during wartime—perhaps the greatest ever. "The Arizona loss occurred as war became evident and her total loss did not match the Rohna's total of 1,138 including British crew members," he added.

In addition to the Bronze Star and the Purple Heart, Brewer holds World War II ribbons including the American Defense Medal, European African Service Medal, Asiatic Pacific Theater Ribbon with 3 battle stars, and the Reserve Medal with 4 devices. He later earned the Air Force Commendation Medal with 3 oak leaf clusters, the Victory Medal, and the China Defense Medal.

In October 2000, Congress officially recognized the heroes of the Rohna.

HMT ROHNA

(Nov. 26, 1943)

British liner/troopship of 8,602 tons, carrying 2,193 passengers, including 1,988 U.S. troops, 7 Red Cross personnel and a crew of 198, sailed from Oran, Algeria, bound for Bombay, India, via the Suez Canal. She joined convoy KMF 26 which consisted of 24 ships and between Algiers and Philloppville, the *Rohna* was hit by a German HS 293 'glider bomb' (the world's first guided missile) dropped from a Heinkel 177 bomber of 11/KG-40. The *Rohna*, crewed by Indian

seamen under British officers and captained by an Australian, was owned by the British India Steam Navigation Company. The ship sank taking 1,015 U.S. troops, 3 Red Cross workers and 120 crew members to a watery death. Between 10:30 p.m. and midnight, rescue ships, including the minesweeper *SS Pioneer*, the Red Cross ship *Clan Campbell* and the *Rohna's* sister ship *HMT Rajula*, reported 'sailing through a sea of floating bodies'. Just over 900 survivors were rescued. Eight of the Heinkel 177s were shot down. (*"Maritime Disasters of WWII"*)

