April 2001

# intercom

*Journal of the Air Force Communications and Information Community*

## Pacific Air Forces Communications and Information

## Delivering Information Assurance to the Warfighter since 1939

# intercom

**Volume 42, No. 4**

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

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

**Editorial Staff**

***AFCA chief of public affairs***
Lori Manske

***Executive Editor***
Len Barry

***Editor***
Tech. Sgt. Michael C. Leonard

***Contributing Editor***
Senior Master Sgt. Frederick Ricker
Pacific Air Forces
Communications and Information

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

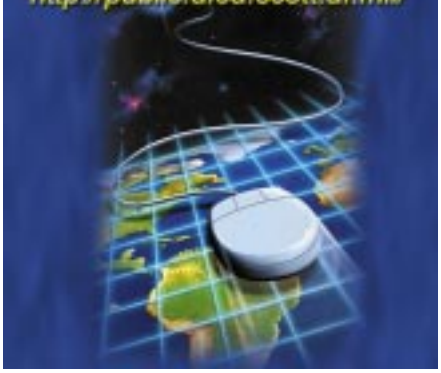
Contents of the ***intercom*** are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or the Department of the Air Force.

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

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

News copy, photos, story ideas and comments may be e-mailed to intercom@scott.af.mil, or mailed to AFCA/XPPA, ***intercom***, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222. Fax is DSN 576-6127 or (618) 256-6127. Editorial staff may be contacted at DSN 779-5690, or (618) 229-5690.


Check out our Web site at:
http://public.afca.scott.af.mil/



## PACAF comm and info


4 PACAF AIRPS provides vital link between overseas and home

10 'Elmendorf out!' marks end of era for global HF station

15 'Team Andersen Update' keeps community informed

18 Morse code site still exists -- Yokota's Global Weather Intercept Program provides valuable service to operational missions

22 Hickam's IM warriors: information excellence in all we do

26 36th CS customers enjoy advantage of Asymmetrical Digital Subscriber Line

28 A day in the life of Wolf Comm can be far from 'typical'

33 Yokota communicators 'Train to Gain'

## IT focus group


37 Server consolidation is key to *One Air Force ... One Network*


## IA Awareness Campaign 2001


38 AFOSI educates members on threats to information systems

40 AFOSI and AFMC team up to provide unique approach to IA

42 Make sure you're not 'bugged'


## in other news


44 Comm and info officers nominated for promotion

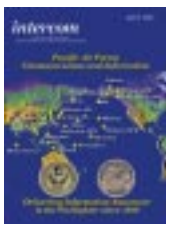
46 Next generation cell phones may impact AF operations


U.S. AIR FORCE CBT

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

### About the cover

**This month's cover focuses on communications and information in PACAF.**



# PACAF commander sees vast improvements, accomplishments in comm and info

**By Gen. Patrick K. Gamble**
*Pacific Air Forces Commander*
*Hickam AFB, Hawaii*

Five months ago, I wrote an article for the *intercom* stating my goal was "to improve efficiency through economies of scale, and reduce our information protection vulnerabilities and costs, while increasing the accuracy and speed of our information flow." As we take inventory of how far we've come, and look to where we're headed in the future, it comes as no surprise to me to see vast improvements and accomplishments of communications warriors throughout PACAF.

Enterprise purchasing allows the command to take advantage of lower prices due to the economies of scale of buying in bulk. Our quick successes with bulk buying initiatives such as AFWAY convinced us to take an even bolder step and develop an enterprise strategy for command-wide purchase of all IT end items. These enterprise initiatives allow us to leverage our limited budgets for increasing information processing capabilities.

Another critical factor in managing our information technology is employing tactics to reduce information protection vulnerabilities and costs. The central point for information protection operations in PACAF is the Network Operations and Security Center. The NOSC is taking an operational approach to managing the PACAF Enterprise by using a Special Instructions to Communicators document and daily Comm Tasking Orders. The SINC document is similar to the SPINS (Special Instructions) document within the operational community, while the Comm Tasking Order is similar to the Air Tasking Order. The SINC is the foundational document used by PACAF communications and information professionals to support operationalizing communications. Our focus is now on applying fundamental operational elements (access, synergy, simultaneity, balance, leverage, tempo, centers of gravity, etc.) across the enterprise to directly enable and support PACAF's mission.

To increase the speed and accuracy of our information flow, we fielded the PACAF Gateway, a MAJCOM-oriented Web interface. The Gateway is operational on both the classified and unclassified networks, and has been benchmarked by another MAJCOM. We believe in using a "Center of Excellence" concept to leverage the talents of our IT resources, whether they're in PACAF or at Air Mobility Command, United States Air Forces in Europe, Air Combat Command, etc. We're also teaming with industry to develop a front-end executive presentation tool to intuitively manage user thoughts by monitoring key strokes, and delivering information direct to their desktop without even a query. Now that's information superiority!

**General Gamble**

Strategic partnering with industry allowed us to take an even more aggressive approach toward improved information flow. Nowhere is this partnering more evident today than with the server consolidation efforts under way in PACAF. We consolidated the mail and file servers at Hickam AFB, Hawaii, and Eielson AFB, Alaska, using a storage area network architecture. I've tasked those bases to move all appropriate functional servers over by Oct. 1.

We're also working with industry to test an initiative to steer the beam on inclined orbit satellites and maintain connectivity with our theater deployable communications equipment. This will help us meet the challenges associated with operational information flow requirements as we reach full operational capability of the PACAF Joint Air Operations Center. Strategic partnering with industry is key to every task we take on in the command, and it will be a foundational part of our strategy to pursue innovation.

Taken together, reducing the cost of information technology, improving information protection capabilities, and increasing speed and accuracy of information flow helps PACAF exploit the capabilities of a complex

See **PACAF** Page 7

# PACAF AIRPS provides vital link between overseas and home

**By Senior Master Sgt. John V. Czumalowski**
*Pacific Air Forces*
*Air Postal Squadron*
*Hickam AFB, Hawaii*

*Photos by Airman 1st Class Tharity Barrett, 374th CS, Yokota AB, Japan*

**Airman 1st Class Stephanie Shields and Staff Sgt. Ernest Bracey process incoming mail from Narita Airport while Japanese Customs Agents randomly select parcels for inspection.**

Despite technological advances that gave us e-mail, electronic bill paying, and Internet shopping, the Military Postal Service remains a vital link between people stationed overseas and their dependents at home. The Air Force organization that represents MPS in the Pacific Theater is the Pacific Air Forces Air Postal Squadron, a field operating agency under the PACAF Communications and Information Directorate at Hickam AFB.

The PACAF AIRPS serves nearly 300,000 patrons through a network of aerial mail terminals and mail control activities on Air Force installations and at major international airports, while processing more than 31,000 tons of mail each year and obligating more than $73 million in mail transportation costs.

Detachment 1, PACAF AIRPS, operates the Seoul AMT, adjacent to Kimpo International Airport, in a facility shared with the Army's 516th Postal Service Battalion. Det. 1 personnel sort and process all military mail entering and leaving the Republic of Korea, while their Army counterparts are responsible for in-country ground transportation of mail. The detachment also operates APOs at Kimhae and Taegu ABs to serve users there.

The largest PACAF AIRPS detachment is at Yokota AB, Japan. Det. 2 is the hub of the Pacific, due to its central location and direct flight capability to any location by commercial means or by Air Mobility Command aircraft. The detachment includes Yokota AMT; Narita MCA, at Narita IAP, Tokyo; and an MCA at Kansai IAP, Osaka, Japan. The Narita and Kansai MCAs serve all military locations in Japan, coordinating with com-

mercial air carriers to ensure mail is moved as quickly as possible. Also in Japan is Det. 3, overseeing Kadena AMT and Naha MCA, which is 22 miles south of Kadena at the Naha IAP. They process mail for Kadena, Marine Corps, and personnel serving on Navy ships in the region.

The most geographically diverse detachment of PACAF AIRPS is Det. 4 in Sydney, Australia. In addition to the Sydney AMT at Sydney IAP, the detachment operates six APOs, with the Sydney APO having the distinction of being the highest APO in the world due to its location on the 58th floor of the building that houses the U.S. Consulate downtown. The APO in Melbourne supports a small U.S. military community, but also serves as the primary means of receiving critical aircraft parts for Defense Contract Management, Australia, which is responsible for refurbishing U.S. aircraft. The Canberra APO is in the U.S. Embassy and serves the military community there, as well as U.S. State Department personnel assigned to the Embassy.

The most isolated APO in the squadron is at Alice Springs in the middle of the Australian outback. It serves DOD personnel stationed at Pine Gap, Australia. The Christchurch APO serves Air National Guard personnel permanently assigned to Operation Deep Freeze, which supports the National Science Foundation and the U.S. Antarctic Program. The Christchurch operation supports an APO at McMurdo Station, Antarctica, and another at the South Pole.

The remaining component of the squadron is Operating Location A in Bangkok, Thailand. OL-A serves military and U.S. State Department personnel throughout Southeast Asia. It provides direct support to the Joint U.S. Military Advisory Group-Thailand and Joint Task Force Full Accounting, and serves as the single service manager during Cobra Gold, the largest annual exercise in PACAF.

The PACAF AIRPS has continually ensured timely movement of military mail for all DOD personnel, their family members, and other authorized users in the Pacific Theater. Its motto, "Serving the Pacific," exemplifies the spirit in which the squadron's men and women continue a proud tradition of excellence. This spirit is best captured by the smiles on the faces of military members when they receive care packages, letters and cards from loved ones far away.

**Staff Sgt. Marc Nickleberry identifies a parcel requiring special handling at the Central Mail Processing Center, Yokota.**

**Staff Sgt. Wendy Newton scans bar codes on mail to determine transit times from dispatch points, as Master Sgt. Alfred Whilite and Yoichi Shimizu unload the mail van from Narita Airport.**

# Computer training center supports Yokota's training needs

**By Daniel Holsapple**
with **Debra Anderson**
*374th Communications Squadron*
*Yokota AB, Japan*

One goal of the 374th Communications Squadron is to provide up-to-date computer training to all Yokota AB customers. The squadron has dramatically expanded a computer training center it reopened just 18 months ago.

The Yokota Computer Training Center was established in mid-1995 and provided Microsoft applications training to all base personnel including Japanese and U.S. civilians. However, due to lack of funding and a perceived lack of need, the center was closed from 1997 until 1999.

The center was reopened temporarily in July 1999 to see if there was a need for the training that would be offered. The 374th CS opted to staff the facility with a civilian lead instructor and the facility director. The center started training the base populace in one classroom that could handle 10 students. They taught standard Microsoft application courses (Word, Excel, Access, Powerpoint and Outlook).

**Debra Anderson teaches a class.**

In addition, a memorandum of understanding was established with the Navy's SPAWAR Information Technology Service Center Pearl Harbor in Hawaii to offer technical certification level training to the base. INTEC PH courses include all certification training for Microsoft Computer Systems Engineer, Novell Certified Network Administrator, and COMPTIA A+ certification. Target audience for these classes are Air Force network control center personnel, workgroup managers, and functional system administrators.

In July 2000, the 374th Airlift Wing approved the comm squadron's request to make the center a permanent fixture at Yokota. Approval was granted to permanently hire the U.S. civilian and two Japanese nationals. During the past year the center director, Debra Anderson, was recognized as the Air Force Communications and Information Professional Civilian of the Year for 1999 for her involvement in making this an outstanding training program. Knowing the impor-

**A Communications Information Transport Systems instructor teaches a TTS Remedy class.**

See **CTC** next page

## CTC

*From previous page*

tance and paybacks of training base users on computer programs, the 374th CS also took an active duty service member out-of-hide to help provide training. In addition to providing people, the squadron expanded the training center from one to three functional classrooms.

From July 1999 to present, the computer training center trained more than 1,700 U.S. military, civilian personnel and Japanese nationals, saving an estimated $700,000 in TDY and training costs.

**Office automation training is provided by the CTC.**

The training program has been structured to provide modern equipment in each classroom, providing students with hands-on capabilities. Additionally structured on-the-job-training, Cisco Academy, Windows 2000 and Office 2000 courses are on the schedule.

Classrooms are also provided to train on-base workgroup managers, functional system administrators, and traveling training teams provided by PACAF.

The 374th CS at Yokota is well prepared to support the computer training needs of Yokota AB well into the future.

## PACAF

*From Page 3*

enterprise. However, the numerous capabilities of the enterprise must be organized and funded as an integrated system to provide PACAF operational commanders and warfighters the ability to attain information and decision superiority throughout their battle space. The Communications Centers of Gravity focus the communications and information professionals on creating the highest levels of information assurance and operational availability for the warfighter. The current CCOGs within the PACAF Enterprise of Responsibility are:

* Senior commanders' situational awareness
* Intelligence collection, processing and dissemination
* Information dissemination management
* Operations battle rhythm

Decision superiority is a powerful contributor to operational effectiveness. However, that contribution can be minimal if operational uncertainties are not collected, assessed and synchronized with the plan. The PACAF SC/A6 is responsible for satisfying theater-level communications and information requirements throughout the command. The NOSC is the organization designated to provide status and oversight of network assets across the theater. My NOSC is a critical link in achieving decision superiority. The NOSC provides real-time situational awareness by flowing critical enterprise events to the PACAF Operations Support Center. The POSC then synchronizes that information with operational status throughout the theater to provide the operational picture. This allows me to make critical theater decisions.

This is just a snapshot of what we're doing within PACAF to seek IT innovation, and pursue it. The time has come to stop chasing technology, and to develop an overarching strategy to harness and exploit the amazing capabilities we already possess and own outright. There's a quote in the book "Network Centric Warfare, Developing and Leveraging Information Superiority" that states "organizations that have been able to fully leverage the power of information and information technologies to develop a competitive advantage have dominated their competitive domains. Those that have been slow to recognize the potential for information and information technologies to transform their organizations and processes, or have failed to go far enough and fast enough to change the way they do business, are being acquired by their competitors or swept away." PACAF has teamed, and will continue to team, with the other MAJCOMs and agencies to dominate and leverage the power of IT.

# PACAF headquarters undergoes major communications upgrade

**By Lt. Col. David J. Gruber,**
**Maj. Michael D. Hales** and **Rich Beese**
*Pacific Air Forces*
*Hickam AFB, Hawaii*

When the Pacific Air Forces Headquarters building was constructed in 1939, it was a barracks housing 3,200 men. Its huge size, almost 500,000 square feet, made it the largest building owned by the military. Its prominence drew an attack from the Japanese during World War II, and their bullet holes still scar the walls of the building. Since the war, the building has gone through many changes in mission. Today it houses the PACAF staff and provides office space for nearly 1,900 people. This dramatic change in mission has compelled a major communications infrastructure upgrade.

Barracks communications capability in 1939 was sparse. Only a few phones per wing were needed. During the intervening years, more telephones were added as offices moved in. Later, computers were introduced. Mechanical rooms and custodial closets were jerry-rigged and became defacto communications closets. These rooms were not environmentally controlled and had minimal power. Wires connecting the floors used the original floor penetrations, which became tightly filled over the years. As the computer requirement grew, the distance to the closets prohibited bringing cable from each workstation back to a switch. Hubs were installed on air vents and other hidden areas in the building, and daisy-chained two and three deep to fill the growing demand. This forced many people to share the bandwidth that one person should have had, and caused network performance problems throughout the building. Individual self-help projects and attempts to upgrade sections of the building over the years provided some relief, but collectively they created a massive headache for maintainers. The building's aging infrastructure could not support yesterday's requirements, let alone today's.

**AC Rooms were used as defacto communications rooms, leaving electronics susceptible to changing temperatures and humidity.**

While the 15th Communications Squadron struggled to augment the building's aging infrastructure, the PACAF commander initiated a program called Operation Kuter. Gen. Patrick K. Gamble decided his staff needed to focus on more than the major command's role of organizing, training and equipping forces as they have in the past. He wanted them to also support the commander of Air Force forces in the Pacific Theater. General Gamble carved out a major area in the heart of the building and created a home for the new PACAF Operations and Support Center. This center integrates the operations activities of all of PACAF directorates and provides COMPACAF with situational awareness of everything that occurs in the theater. The general also established a new air operations group to operate the POSC and act as the cadre for any action that might occur in the theater. The POSC formed the nucleus of the PACAF staff's support to military actions ranging from humanitarian relief, to non-combatant evacuations, to war.

General Gamble recognized this approach would not be cheap. He put together a funding plan that included not only upgrades to the facility, but a major upgrade to the communications infrastructure. The general knew his ability to command and control forces in the theater was dependent on robust communications between his directorates. Operation Kuter has absorbed much of the 15th Communications Squadron's resources. The squadron has begun constructing real communications closets on each floor in every wing. These closets provide an environmentally controlled area and provide physical security to protect against tampering. The squadron has installed cable trays above the false ceilings to allow cable to be run directly from the cable closet to each wall jack. The new cable eliminates daisy-

**Lightwells in the corners of the building have become 'cable risers' to the floors in each wing. Each lightwell services multiple wings.**

chained hubs and provides a minimum of 100 megabytes of bandwidth to each user. Thanks to the help of the 130th Electronics Installation Squadron, the building's protected distribution system has been expanded and alarmed. PDS provides the conduit used to extend Secret Internet Protocol Router Network service throughout the PACAF staff. It also includes an alarm console in the network control center where communications squadron technicians can monitor PDS status.

As stated earlier, the POSC resides in the heart of the building. Once complete, the floor immediately beneath the POSC will house the 15th CS Network Control Center and the PACAF Network Operations and Security Center. All of the servers supporting PACAF, as well as the building's telephone switch, will also be located on this floor. The 15th CS has already consolidated e-mail and file storage at Hickam on clustered super servers backed by a huge storage area network. After the NCC and the super servers move into the new facility, PACAF intends to mirror the information stored on the headquarters SAN at another location on base. This will increase the reliability of PACAF's information and ensure the staff has access to it at all times.

During the construction, the 15th CS made significant improvements to its existing NCC. It developed a daily stand-up briefing that has become the model for the command. It officially deactivated the help desk and created a true control center where technicians, under direction of a crew commander, operate the Hickam network. Monitors mounted in the control console provide immediate status of the classified and unclassified networks. Other monitors indicate the status of all servers controlled by the NCC, and a special alarm screen is activated if a server breaks any predefined operating parameters. The 15th CS manned the control center with experienced technicians rather than new people. This initiative, coupled with an extensive work group manager training program, has led to a dramatic decrease in the number of open jobs, and a corresponding increase in customer satisfaction. Now when someone calls the NCC, his or her problem is resolved, and not logged into a database for someone else to work later.

Operation Kuter has ushered in an exciting time for Hickam AFB. Headquarters PACAF will never be the same. On Dec. 7, 2001, Army Air Corps veterans of the attack against Pearl Harbor will return to Hickam AFB for the 60th anniversary. Although they'll visit the building that some of them once called home, they'll find something far different from what they remember. The bullet holes will still be in the walls, but the heart of the building will have changed drastically. What was once a large, but ordinary, barracks has become home to a truly operational headquarters staff.

**Dedicated comm rooms are designed with rack space, overhead cable trays, and room to grow. All are environmentally controlled.**

# ‘Elmendorf out!’ marks end of an era for global HF station

**By Master Sgt. Mark Hoffmeyer**
and **Staff Sgt. Lavette Williams**
*3rd Communications Squadron*
*Elmendorf AFB, Alaska*

As of March 1, the Elmendorf global high frequency radio station was no longer manned. Radio operators and maintainers were reduced by 28 positions with implementation of Scope Command, which is the most recent upgrade to the Air Force’s worldwide HF radio network. It replaces the 1980s vintage Scope Signal III system that gave Strategic Air Command continuous HF radio communications for positive control of airborne forces worldwide. Scope Signal III was installed at Elmendorf in 1985 to augment even older equipment already in place. One thing that hasn’t changed is the mission. Scope Command provides continuous, reliable, two-way communications to all Department of Defense aircraft, ships and ground agencies in the North Pacific and Arctic regions.

Performing this mission was a long and proud heritage of the men and women of the 3rd Communications Squadron, whose positive impacts were felt from the ‘50s until last month. Now the same services are provided from a facility thousands of miles away, at Andrews AFB, Md.

**Tech. Sgt. Mark Wirick mans new Scope Command console.**

**Historical background**

With the 1867 Alaska purchase and discovery of gold came the need for better communications to help secure the frontier and gold camps. In those days, it could take up to a year for a message to pass between Alaska and Washington. This situation launched Alaska’s continuing quest for faster and more reliable communications.

**Airman 1st Class Donna Stevens monitors Scope Command functions.**

In 1900, Congress approved the Washington-Alaska military cable and telegraph system, establishing communications from Alaska to Seattle. Later WAMCATS led to development of early wireless (radio) stations. These new systems were so effective that widespread use by commercial customers caused Congress to authorize collection of fees for connecting commercial carriers. This network was known as the War Department’s Alaskan Communications System. In 1971, the system was sold to RCA-Alascom, later shortened to Alascom, which provided commercial and residential communications to all of Alaska. Today Alascom is part of a bigger communications company – American Telephone

and Telegraph.

In the 1950s, it became apparent the military Alaskan Communications System could not sustain both military and commercial needs. A new radio system called White Alice was developed in 1958 to meet communications demands of the Cold War. It greatly improved Alaska's air defense posture and marked the beginning of HF communications for the 3rd Communications Squadron's global radio station. White Alice beamed radio signals upward from a parabolic transmitting antenna, bouncing them off a layer of the earth's atmosphere, and back down to a receiving antenna hundreds of miles away. The system enabled remote elements of Alaska's military to contact each other. Its primary drawback was poor radio propagation caused by interference from aurora borealis. The Elmendorf AFB global HF radio station was located on the far north side of the base, overlooking the Cook Inlet, and, on a clear day, within view of Mount McKinley.

**Senior Airman Tanya Griffeth enters data into the Scope Command system.**

Surrounded by acres of antennas, global radio operators diligently provided many vital services, primarily to airborne aircraft. Encrypted emergency action messages, aircraft advisories, Air Force One presidential support, and in-flight emergency coordination were the main military missions supported. For example, an encoded EAM could order a submarine to launch a missile on a given target. The action movie "Crimson Tide" provides a dramatic illustration of the function of EAM. For radio operators, the phone patch was one of the more enjoyable services because it involved direct contact with aircrews. According to Staff Sgt. Mark Cisco, an Elmendorf global radio operator since 1996, "We were obligated to provide almost any requested support, so if a pilot wanted the score of a World Series game, I gave it to him." Most of the phone patches, however, dealt with weather conditions, landing and refueling information, and even billeting arrangements. Airman 1st Class William Garrett, an operator since 1999, recalled the job satisfaction of coordinating support for a rescue mission for a group of sightseers stranded in the interior. He gave rescuers a discreet frequency so no one could interrupt them, and helped them communicate with the group. The station's normal 24-hour radio traffic load averaged about 200 phone patches, 400 HF contacts, and 540 advisories a month.

**Elmendorf today**

Elmendorf is one of 14 radio stations worldwide coming online with this new computer-based system from Rockwell-Collins Co., under the Scope Command installation project. The new system supports the same mission, but uses state-of-the-art, commercial off-the-shelf equipment with solid-state high-power transmitters, remote control, automatic link establishment and fiber optic links.

The new system provides a major cost saving by consolidating radio operators at the central network control station at Andrews AFB, Md. CNCS operates Elmendorf's equipment – and 13 other radio stations worldwide – by remote control. The system reduces the total number of radio operators and managers, and saves the costs associated with maintaining 14 separate stations. Elmendorf lost 22 radio operators and six maintainers, while Andrews picked up nine operators. CNCS can send and receive radio traffic as well as if they were located at Elmendorf. In fact, one of the 14 operator consoles at Andrews is designated "Elmendorf."

Scope Command's incorporation of the automatic link establishment function affords high tech to HF radio users. Each priority user gets an ID number, and when a CNCS operator enters that number, the Scope Command terminal automatically searches and links to that user on the frequency with the best quality and reliability, causing the customer's radio to "ring," and establishing an HF communications link.

On March 1, a chapter of history came to a close when Col. Douglas Fraser, 3rd Wing commander, ordered the 3rd Communications Squadron's radio operators to perform the final manned radio broadcast and relinquish control of Elmendorf airwaves to CNCS.

The end of an era was marked with the final transmission of the words, "Elmendorf out!"

# PACAF replaces Adak Island TACAN, with a lot of help from friends

**By Staff Sgt. Liam J Clancy**
*Pacific Air Forces*
*Hickam AFB, Hawaii*

What do you do when you learn that a critical navigational aid system in direct support of civilian aircraft and military warfighters is slated for decommissioning? Team PACAF answered that question in short order this past fall by acquiring, transporting and installing a tactical air navigation system at Adak Island, Alaska. Typically, a project of this magnitude would have taken two years to plan and execute. Team PACAF, spearheaded by Headquarters PACAF/SCNM and HQ PACAF/DOYA were able to streamline and complete the enterprise in six weeks at a fraction of the estimated $2 million cost.

How did they manage this Herculean task? Let's say they got by with lots of help from their friends. Typically, a major command would request a system, the installation would be engineered and an installation package would be developed. This system would then be ordered from the manufacturer and the command would wait 12 months or more for construction and shipment to the project site. The process would usually take the better part of two years. With the Navy TACAN scheduled for removal in only six weeks, Team PACAF did not have 24 months to wait. Winter in the Aleutian Islands was fast approaching, and other options had to be explored.

Why is Adak so important to the Air Force? It's because of its strategic location. Take a look at a map of Alaska and you'll find the Aleutian chain stretches westward from mainland Alaska. Adak is halfway out, approximately 1,300 miles from Anchorage. Its location is nearly equidistant from Tokyo and San Francisco. This places it at a crucial point in both commercial and military flight routes across the Pacific. Without the TACAN to guide aircraft to Adak, pilots experiencing difficulties on those routes would have nowhere else to go.

What is a TACAN? It's a ground-based, navigational beacon that radiates between 400 and 5,000 watts in the ultra high frequency range. Aircraft up to 200 miles away can interrogate the TACAN and receive a reply specifically coded for that aircraft. Embedded inside this reply train is all the information the aircraft will need to ascertain the direction and exact distance to the TACAN site. This allows the aircraft to fix its position relative to the TACAN in any weather situation. Without this beacon, aircraft approaching Adak would have a difficult and dangerous time picking their way between the mountains and volcanoes that surround the island in hopes of locating its runway.

Team PACAF brought their problem to the good folks at the Air Force Materiel Command. With their help, a spare TACAN was found sitting in an unused classroom at Keesler AFB, Miss., Technical Training Center. AFMC provided this TACAN to PACAF at no charge, and even volunteered to dismantle the TACAN with assistance from one of their engineering and installation teams. Master Sgt. Todd Carlin, PACAF's special maintenance team leader, flew to Keesler to test the system's serviceability and supervised the removal operation. Even the 81st Training Squadron got involved when it was discovered there was no technical data available for the system. The folks at the technical school dug around and found an extra set of books that they provided to support the project. Sergeant Carlin, with the help of contract maintenance technicians, identified problems with the system prior to its removal. He then packed a "bag of tricks" which included tie wraps, fuses, spare connectors and other odds and ends to eliminate potential show stoppers. Sergeant

**Members of the 738th Engineering and Installation Squadron prepare the TACAN antenna for removal at Keesler AFB, Miss.**

Carlin knew all too well that a quick jaunt to Radio Shack would be out of the question 900 nautical miles off the coast of Alaska.

With the help of the 738th E&I squadron at Keesler AFB, the TACAN (and its rather large and ponderous antenna system) was removed in just a few hours and delivered to the transportation folks for crating. The 3,000 pound system was then packed on a flatbed and hauled from Keesler AFB to Travis AFB, Calif., in only three days. Next, the team at Travis aerial port took responsibility and provided military airlift to Elmendorf AFB, Alaska, for delivery to the 611th ASUS, just two days later. Transporting the system from one end of North America to the other was the easy part. The greatest challenge was yet to come.

How would Headquarters PACAF get the TACAN and its five-man installation team to Adak Island? Local commercial air transportation was too small to carry the cargo, and regularly scheduled military flights to Adak did not exist. Again team PACAF got by with a lot of help from their friends.

Sept. 22, at 7 a.m., a C-130 from the 517th Airlift Squadron took off from Elmendorf AFB, bound for Adak Island, Alaska. On board were the TACAN system, a five-man installation team and several hundred pounds of spare parts and test equipment. Five weeks after the project started, installation was ready to begin.

The team that flew to Adak included Tech. Sgt. Tim Lilly and Staff Sgt. Chris Casey of the 611th ASUS, Master Sgt. Todd Carlin and Tech. Sgt. Gerald 'Stu' Johnson of the PACAF Special Maintenance Team, and Staff Sgt. Liam Clancy from HQ PACAF/SCNM. The 611th ASUS would accept responsibility for the TACAN once the installation was completed. The 611th ASUS has a large and varied mission with sites from Eareckson AFS, Shemya, at the tip of the Aleutian chain to Point Barrow on the North Slope. If there's a site in Alaska that is "not fit for man nor beast," it most probably belongs to the 611th ASUS.

The first order of business upon arriving at Adak was to check the cargo and make sure nothing got damaged during transportation. Desperation and disbelief gripped the installation team when they found that the antenna had slipped inside its 14 foot by 7 foot by 7 foot crate. This could have been a real "show stopper." The team quickly rigged a temporary antenna-lifting sling and raised the unit for inspection. Luckily no damage was done. The team carefully set the antenna back into the shipping cradle and secured it for the arduous journey up Beacon Hill to the TACAN site. With only seven days remaining until the Federal Aviation Administration flight inspection, time was of the essence.

Next, the team inspected the installation site to begin the process of installing the Air Force system. Because of the time constraints, the Air Force TACAN would need to be installed before the Navy removed theirs. This was tricky due to the congestion of sensitive equipment inside the building. This building

**Contractors prepare the Navy antenna for removal, Adak Island, Alaska.**

housed not only the Navy TACAN, but also a FAA navigation beacon and a land mobile radio repeater. With tremendous help from the Adak community in metals fabrication, tool and heavy equipment support, the installation proceeded smoothly. The Air Force system was installed and tested in only two days. Once the Navy removal team arrived, everyone pitched in to help remove the Navy TACAN and antenna system. The Navy team was instrumental in getting the Air Force antenna lifted into place and the Air Force team secured it against the vicious winds of Beacon Hill.

Weather and mechanical problems delayed the flight inspection by three days. Finally, Oct. 2, a mere six weeks after the project started, the FAA certified the newly installed Air Force TACAN as operational, and the northern flying route was once again safe for use by commercial airliners and our military warfighters.

A two-year project had been completed in record time, thanks to a lot of help from our friends. Without the can-do attitude and cooperation between Air Force commands, the Navy, and the people of Adak Island,this project would never have been completed in only six weeks at an impressive savings of more than $800,000.

# Strategic planning: regular way of doing business at 35th CS

**By Master Sgt. Neil McComsey**
*Superintendent, Plans and Implementation Flight*
*35th Communications Squadron*
*Misawa AB, Japan*

After taking command of the 35th Communications Squadron in August 1999, Maj. Von Gardiner and his staff set a course to make command, control, communications and computer systems planning a regular part of doing business. Major Gardiner gave responsibility for strategic C4 planning to the plans and implementation flight. Almost 18 months later, the 35th CS and, more importantly, the 35th Fighter Wing and Misawa AB, are seeing a significant return on investment.

As part of the C4 planning effort, the 35th CS totally revamped its processes. A new C4 project database was designed. It captures data from a variety of sources and incorporates disparate information into an integrated databank of C4 requirements, projects, plans, civil engineering and major construction programs, installation records, long-range C4 blueprint plans, network architecture and configuration control documentations, and support agreements. The result is a user-friendly application to track current C4 assets and infrastructure, and to project future C4 requirements and prioritize them based on funding and mission needs.

During the 2000 Pacific Air Forces Unit Compliance Inspection, this C4 application was noted as a "strength." Lauded by Col. Ronnie Hawkins, PACAF CIO and director of communications and information, the application is being modeled for use command-wide. Basically, the 35th CS was tracking all forms of C4 services and architectures in different work centers and using divergent media. The objective was to bring all relevant information into one usable system to track current C4 systems and actively plan for future needs. While still a work in progress, the squadron already realized a return on this investment in the form of customer satisfaction. The wing is better postured to vie for scarce funds and leverage existing assets—it now deals with facts when it comes to what C4 systems and services are needed, why and when.

Incorporating C4 requirements into strategic planning set into motion additional process improvements, including establishment of standard solutions for common computer hardware and software. These standard solutions help warfighters plan for and procure supportable computers, software and other peripherals in half the time it took to process a separate requirement. Customers no longer have to submit a separate AF Form 3215, C4 Systems Requirements Document, for each PC or printer purchase. The transition to purchasing computers in bulk via AFWAY was nothing new for Misawa, since the 35th FW started buying standard systems in bulk in September 1999. Streamlining the entire business process for computer acquisition allowed Misawa to leverage its limited funds and increase buying power.

After getting its hands around current and future C4 requirements, the 35th CS needed to develop a formal, repeatable process to pass requirements to the base senior leadership and get their support. A three-tiered process was established in April 2000 to ensure leaders had perfect situational awareness of all significant C4 issues. The first tier consisted of user working groups like the LAN configuration control board, comprised of unit computer managers, workgroup managers, and other IT-savvy customers. Major C4 projects, issues, and unfunded requirements were compiled by user working groups and communicated to the C4 Working Group, the second tier of the planning hierarchy.

The C4 working group is chaired by the 35th CS commander and consists of respective unit resource advisors, IT managers, and squadron commanders. After the C4 working group validates and prioritizes C4 requirements, they are passed to the C4 Forum, chaired by the wing commander or vice commander and including the group commanders as voting members.

Timing is everything, and it's no accident that the C4 requirements process timelines parallel the base's financial process -- financial working group and financial management board. Last fiscal year this three-tiered process proved instrumental in garnering base-wide support and funds for many C4 requirements including a major ISDN switch upgrade, two digital subscriber line installations, trunk-capable radios, network control center server upgrades, network infrastructure upgrades for both NIPRNET and SIPRNET, and wing-wide computer, printer, and software upgrades. Misawa is better able to point its limited funding resources at agreed upon C4 targets.

As a result of this strategic planning effort, the 35th CS also realized a significant return in the area of new construction. By partnering with local civil engineer planners, it identifies C4 requirements associated with major construction during the design review phase—two years before project completion. The squadron can ensure quality C4 services are in place for all new facilities as soon as the first occupant sets foot in the door. Close coordination with the civil engineers, the custom-

See **STRAT PLAN** Page 21

# ‘Team Andersen Update’ keeps community informed

**By 1st Lt. Quintin Tran**
*36th CS Support Flight Commander*
*Andersen AFB, Guam*

The 36th Communications Squadron at Andersen AFB produces a 10-minute television show called “Team Andersen Update.” This news program is a tool for the wing commander to get information out to the wing quickly and effectively. It also keeps the Team Andersen community up-to-date on happenings around the base.

“Team Andersen Update” is aired twice a day on the base commander’s access channel. Topics range from DV visits to exercises and contingencies, such as the latest airlift relief effort for earthquake victims in India.

A two-person team of videographers from the support flight, Staff Sgt. Jon DelMonico and Senior Airman Pedro Jimenez, shoot and edit all the material for the show and write the script. “Team Andersen Update” is an additional duty that the 36th CS goes above and beyond to produce. The show is done in conjunction with its usual visual information duties.

With the recent loss of the broadcaster position, Sergeant DelMonico used an idea to allow different members of Team Andersen to be guest hosts. This puts Andersen’s best airmen in the spotlight.

The video section works closely with the wing public affairs office to stay on top of breaking stories on the base. “It’s a total team effort to get the stories, put the show together, and then have it aired,” said Lt. Col. Kurt R. Fox, 36th CS commander.

**‘Team Andersen Update’ videographer Senior Airman Pedro Jimenez and Staff Sgt. Jon DelMonico (seated).**

After events are identified for the show, the video team documents them. All footage is taken back to the flight, digitized, and edited with a state-of-the-art, non-linear, computer-based editing system. The stories are put together with sound and music, and voiced over to give it a TV news style. Air Force commercials and community announcements are spliced in to promote retention and enhance community awareness. After the stories are put together, the script is written and the host is brought into the studio to videotape scenes.

The 36th CS will continue to produce “Team Andersen Update” because it serves the base community and is a valuable tool for the wing commander.

# *Wolf Comm gives a voice to the Pack*

**By Maj. Dennis Simpson**
*8th Communications Squadron Commander*
*Kunsan AB, Korea*

You know from the time you step off the Patriot Express rotator that being a member of the 8th Fighter Wing, the "Wolf Pack", will be special and different than any other assignment. The first thing you hear is music is blasting and the wing commander and other Kunsan senior leaders enthusiastically greet you. You're whisked from the flight line to the main reception area, where all of the base's squadron commanders, first sergeants, and others form a line and welcome you to the Wolf Pack. Once everyone's settled, the wing commander, Col. Philip Breedlove (affectionately known as the Wolf) introduces you to Kunsan. The 11 words of the 8th FW mission ring in your mind when the Wolf walks off: "Defend the base, accept follow-on forces, and take the fight North!"

Welcome to one of the U.S. Air Force's last true remote front-line fighter bases. Our mission drives everything we do. Everyone in processes and is ready to fight within two days after arrival. So how does the 8th Communications Squadron, Wolf Comm, fit into that picture?

The first, and most important, part of our mission is to "defend the base." Our primary support for this part of our mission involves firing up portions of the secure network, doing final operational checks on the communications at alternate operating locations, and keeping the rest of our systems in fighting shape. You'll also see us stringing concertina wire and putting camouflage on defensive fighting positions at all three of our main compounds on base.

Members of Wolf Comm have lots of experience building DFPs after filling about 12,000 sandbags to rebuild all 11 of them. We spend a lot of time in them too. In the last 12 months, Wolf Comm members grabbed their M-16s and manned the DFPs for eight full-scale, 24 hours-a-day, week-long wing exercises, including Foal Eagle, a peninsula-wide exercise involving U.S. soldiers, sailors, airmen and Marines, and Republic of Korea forces. This year's Foal Eagle was the largest base defense exercise in the Department of Defense. The Wolf Pack also faced an Operational Readiness Inspection in May and another ORI last month.

The second part of our mission is to "accept follow-on forces". The Wolf Pack can't fight the war alone. We practice accepting follow-on forces by integrating elements of the Dragons of the 607th Combat Communications Squadron from Camp Humphreys into the Wolf Comm team. We've also stockpiled networking and telephone equipment to enable us to quickly increase base services for thousands of people who would descend upon Kunsan in a real war.

The third part of our mission is to "take the fight North". Wolf Comm supports that part of the mission by ensuring continued availability of the base's command and control systems. We've installed an extensive classified network (180-plus workstations) that connects all squadrons. There's no doubt in anyone's mind that "there are no bombs without comm."

Wolf Comm work is challenging. One "Wolf year" is like three anywhere else. We overcome 100 percent yearly turnover in personnel and play a key role in the almost monthly exercises, while providing uninterrupted service to the 2,400-plus members of the Wolf Pack. People must get spun up in no time. You're considered an "old hat" after you've been here a week. For example, one of our newest members stepped off the plane on a Friday, was in the primary unit control center tracking simulated unexploded ordnance and chemical sweeps, and making warning announcements for SCUD attacks for an exercise two days later, and executed her job to perfection.

One might believe this high ops tempo, combined with being away from loved ones for a year, automatically leads to low morale. Not so. Morale and esprit de corps of the Wolf Pack is arguably higher than for any other wing. Being able to fight a war from this base is our primary focus. People who say Kunsan is a bad tour haven't been here. From the Post Office to the Network Control Center, being a part of Wolf Comm is a special and unique experience you'll never forget. Wolf Comm! Voice of the Pack! Hooah!

# 18th CS supports base elementary school

**Senior Airman Vanessa Davis helps out by collecting money from Kadena Elementary School students for their book purchases.**

**Story and photos by Senior Master Sgt. Clarence L. Mathis**
*18th Communications Squadron*
*Kadena AB, Japan*

"Dot com" has filled the classrooms of Kadena Elementary School thanks to the men and women of the 18th Communications Squadron.

As of January, 100 percent of the classrooms at Kadena Elementary School had Internet access for students in first through six grades.

In March 2000, Kadena Elementary School received more than 50 computers with which to develop a computer laboratory for its students. With a staff of only two computer technicians at the school, it was virtually impossible to quickly get all the computers set up and operational for the students.

The 18th Communications Squadron heard about the task and rose to the challenge. With only one week's notice, over 30 volunteers from the unit rolled up their sleeves on a Saturday morning and pitched in.

Spearheaded by Senior Master Sgt. Clarence Mathis, Information Systems Flight superintendent, and Master Sgt. Steven Lundmark, EMSEC manager, volunteers worked with enthusiasm as they unpacked and set up the computers and peripheral devices and sorted software documentation in only 45 minutes.

"We expected the task to take four hours to complete," said Sergeant Lundmark.

Efficient organization was the key to a successful set-up. Sergeants Mathis and Lundmark completed a site survey and designed specific tasks for the volunteers prior to starting the project. "It went like clockwork," stated Sergeant Lundmark.

The quick computer installation gave the volunteers an additional three hours to put to good use. They were able to help out in other school improvement projects. For example, after an on-the-spot training session from squadron volunteers, the school's computer technicians were able to convert the 50 new desktop computer systems to tower systems in less than 30 minutes.

The time spent at Kadena Elementary was a huge success. Some squadron volunteers felt a more personal connection because of their accomplishments, particularly since many of their children are students who will benefit from these improvement projects. But whatever the reason that brought out the 18th CS folks, the 18th CS is truly proud of their dedication, flexibility, efficiency, teamwork and enthusiasm.

The support for the school does not end with computers. In fact, recently, Kadena Elementary requested volunteers to help out with their book fair. The men and women of the 18th CS remarkably filled the request in only two hours.

The spirit of service and teamwork is alive and strong in the unit. To emphasize its commitment, Lt. Col. Harold McKelvey, 18th CS commander, signed a partnership declaration that pledges the squadron's continued support of Kadena Elementary School. Going beyond the call of duty is all in a day's work for the 18th CS. Whether it's on the job or working with the community, service before self and excellence in all they do are what drive the men and women of the 18th CS.

**Members of the 18th Communications Squadron assist Kadena students on computers.**

*Morse code site still exists*

# Yokota's Global Weather Intercept Program provides valuable service to operational missions

**By 2nd Lt. Catercia Isaac**
with **Tech. Sgt. Denis McMonagle**
*374th Communications Squadron*
*Yokota AB, Japan*

**Kazunori Koyanagi transmits a formatted weather message to Tinker AFB, Okla., via the Weather Intercept Control Unit.**

In this age of global satellite communications systems and high-speed data connections, there are stations in the world that still rely on the 160-year-old technology of Morse code to communicate. Why? Because Morse code requires the simplest of equipment and maintenance, takes up little bandwidth and is understandable through almost any kind of interference.

One such station is the Owada High Frequency Receiver Site assigned to the 374th Communications Squadron, Yokota AB. It is a Global Weather Intercept Program station, about 15 miles from Yokota. The site is responsible for maintaining radio receivers for the weather intercept mission as well as other types of receivers that support various Department of Defense missions. Owada collects foreign weather data that is not available from the World Meteorological Organization Global Telecommunications System. The data is collected by intercepting weather radio broadcasts sent in Morse code from selected locations.

**Toyoma Kishida fine tunes a signal on a Racal receiver.**

The DOD GWIP is a joint Air Force and Navy weather program that determines whether mission-impacting weather conditions are occurring throughout the world. The intercepted weather data is compiled and transmitted to the Air Force Global Weather Center and the Fleet Numerical Meteorology and Oceanography Center. These units analyze, develop and forecast the data that supports day-to-day operations within DOD, as well as the operations of combatant commander-in-chief's deployed forces.

The flow of data from interception to final analysis begins at the GWIP station. The station is assigned various geographic locations based on the location of the transmitting target and the commander-in-chief's requirements.

See **WEATHER** next page

# Japan fiber optic upgrade 40 years in the making

**By Tech. Sgt. Gerardo Salazar**
with **Staff Sgt. Jonathan Harris**
*374th Communications Squadron*
*Yokota AB, Japan*

One of the 374th Communications Squadron's goals is to make continuous improvements that make it easier, quicker and less expensive for customers to get first class service. Over the last 40 years they have done just that. Working with the Defense Information Systems Agency, they are on the verge of replacing 21 microwave towers throughout Japan with high-speed, high-capacity, less expensive fiber optic cables.

**The early years**

*Japan Tropospheric-scatter System*

In 1961, the Department of Defense, through a U.S. Army contract, bought a tropospheric scatter communications system from the Nippon Electric Company. Its purpose was to replace the existing, inadequate intra-theater communications network serving Japan, Korea and Okinawa. JTS consisted of 17 sites in Japan and one in Korea, and was completed in 1963 at a cost of $11 million.

*Kanto Plain Communications System*

In November 1982, Headquarters Air Force Communications Service began Kanto Plain Communications System implementation. This initiative replaced JTS and provided analog microwave to 24 sites. By May 1983, the KPCS had reduced to 17 sites.

To further streamline communications, increase throughput, and reduce costs, a move from analog to digital microwave was programmed. This enabled each link to support 45Mb/sec. The transition started in June 1986 and was completed in November 1990.

**The upgrade to fiber**

Better, more dynamic communications is a continuing goal throughout the military and civilian communities. JTS and KPCS didn't meet the increasing requirements for bandwidth and speed. The dynamics and reliability of fiber optics made it the best media to support requirements. It's much less expensive to operate and maintain. Today, a single strand of fiber optic cable has a capacity of up to 400 Gbps (up to 25,000 times more than troposcatter or microwave systems).

*Defense Information Systems Network upgrade*

Leased fiber optic cables now connect the last few DISN sites in Japan. The first advantage is obviously bandwidth. A second advantage is dynamic routing and restoration capability of the ATM infrastructure being implemented. This provides capability to immediately find alternate paths for circuits if a connection is lost between sites. The goal is to reduce, if not eliminate, communications outages. The scalability of the upcoming network is by far its greatest advantage. While microwave technology limited the 374th to maintaining one network strictly for communications within the Kanto Plains and a separate network to reach distant stations, the use of ATM and fiber will allow it to be part of the unlimited worldwide network.

The 374th CS is working with DISA to complete this upgrade. The 374th will still operate and maintain the DISA Facility Control Office for day-to-day operational maintenance of all the link sites on mainland Japan, from Misawa AB at the northern tip, to Sasebo Naval Base at the southern tip.

The project is scheduled for completion in May. The current system has been 40 years in the making, but is just the next step in the 374th CS's goal of better and faster service for all its customers.

---

## WEATHER

*From previous page*

The data received at GWIP stations is raw formatted serial data. Once data is received it's relayed to the Weather Intercept Control Unit at the GWIP station. The data is then processed, reformatted and sent to Tinker AFB Weather Switch, where it becomes part of the next day's weather report. GWIP provides real-time, global-scale information that increases the probability of a successful mission.

**A Racal receiver**

Radio operators monitor the Morse code in five-person, 12-hour shifts to provide the 24 hours a day, seven days a week, 365 days a year coverage necessary to collect the data. Owada is the only GWIP station in the western Pacific region and provides a valuable weather service to missions in the area.

# Elmendorf's air traffic control tower goes high-tech

**By Master Sgt. William G. Boyce**
*3rd Communications Squadron*
*Elmendorf AFB, Alaska*

Until recently, the computer revolution had little influence on how air traffic control personnel performed their job. While most facets of the Air Force, from aircraft maintenance to smart munitions, had seen computer chips change the way things were done, radio technology and the associated voice circuits air traffic controllers relied on had not changed much for 25 years. At Elmendorf, this is no longer the case. Last summer, the 3rd Wing's air traffic control tower made a quantum leap into the 21st century by installing a new enhanced terminal voice switch and a dedicated fiber optic communications link.

ETVS was programmed for installation at the base as part of a Department of Defense and Federal Aviation Administration program aimed at upgrading air traffic control communications around the globe. The new microprocessor-based digital voice switch gives air traffic control personnel touch-screen selection of up to 30 ground-to-air and ground-to-ground radio channels and 40 independent telephone lines.

With a firm installation date, it was evident that this sophisticated technology and equipment would stand out in sharp contrast with a tower designed in the 1950s. A tiger team, composed of personnel from operations and the support group, quickly formed to study the feasibility of remodeling the air traffic control tower cab and upgrading communications infrastructure to better accommodate ETVS. With funding approved, personnel from the 3rd Operational Support, 3rd Communications and 3rd Civil Engineering squadrons accelerated their efforts to custom design a wraparound console, upgrade facility wiring, and replace a problematic underground lead-sheathed telephone cable with a state-of-the-art fiber optic link.

The renovation project was completed in 50 days and resulted in a facility custom-tailored for a system that is light-years ahead of its predecessor. ETVS replaced the 20-year-old manually switched OJ-314 communications consoles in the tower cab, as well as the radar final control facility. The new equipment incorporates a standard PC maintenance terminal for troubleshooting, diagnostic testing, and expeditious defect isolation. Fault analysis that used to require communications personnel hours or days to accomplish under the old system is now performed in seconds. In addition to running lightning quick diagnostics, the maintenance terminal is used to program individual operator positions. Where the old system relied on manually positioned and sometimes confusing patch cords, ETVS can be custom configured or re-configured easily with simple keyboard commands. Computer touch-screen technology has taken the place of manual push-button selection of radio and telephone circuits.

**Senior Airman Victor Davis, 3rd Communications Squadron, checks status of the enhanced terminal voice switch from the maintenance position.**

The next phase of the project was to interface the new switch to the base telephone network and remote ground-to-air transmitter and receiver site. This could have been achieved by simply making necessary connections on in-house telephone demarcation blocks. However, to mate a $250,000 digital switch to the GATR site using an old copper cable buried shortly after the Korean conflict, somehow just didn't seem to be the right thing to do. Aside from being old and inherently

See **TOWER** next page

## TOWER

*From previous page*

noisy, existing cable was prone to catastrophic seasonal outages during inevitable spring thaws. Personnel in the 3rd Communications Squadron's plans and implementation flight went to work on a high-tech fiber optic solution. The result was a fully redundant fiber optic link capable of handling 44 simultaneous audio channels and 22 key lines between the air traffic control tower and the GATR site. Unlike the copper it replaced, the fiber is virtually noise-free, and the resultant audio, when reproduced, is crystal clear. The system was designed with redundant fiber optic transmitter cards and power supplies, with a feature that senses a module failure and automatically switches to a standby module. In addition, a computer maintenance terminal continuously monitors the entire system. Should a failure occur, it triggers an audible alarm and sends an error message to the display terminal to assist maintenance personnel in troubleshooting.

**Air traffic controller Airman 1st Class Beth Simmons guides a pilot on final approach.**

The level of technology involved in Elmendorf's new air traffic control communications equipment may not be cutting-edge, when compared to the latest generation fighter aircraft or weapons systems. However, when compared to the equipment it replaced, the ETVS and fiber optic link represent a major technological leap in voice processing technology. Air traffic control and radio maintenance personnel at Elmendorf have to admit that the computer revolution has finally made its way into their respective jobs in a big way.

---

## STRAT PLAN

*From Page 14*

ers, and the government of Japan on construction programs has helped save the wing and the U.S. Air Force millions of dollars by incorporating C4 requirements into the government of Japan-funded construction program.

This past fiscal year a multi-million dollar, multi-use support facility and multiple Navy facilities were completed and fully equipped with modern network, telephone and cable TV infrastructure. Future construction projects have already been earmarked for new C4 systems, to include a new fire station and officers' club. To top off this cooperative effort, the 35th CS coordinated with 35th CE on a $20 million government of Japan-funded C4 infrastructure upgrade project. This project will provide much needed replacement of the base's 45-year-old telephone and copper cable as well as provide fiber optic cable to sections of the base without fiber optic connectivity. Bottom line, customers no longer move into new facilities and scream for communications support as they walk through the door -- all the comm is already there.

Strategic planning efforts didn't stop there. The 35th CS compiled complete documentation of the base's fiber network (local area network) using visio drawings and digital photos. It is better able to track fiber usage and plan for upgrades as fiber paths become saturated. As an added benefit, maintenance troubleshooting is made easier by having readily identified fiber records. All new network installations are documented to provide a historical record and continuity.

The squadron has taken its planning show on the road, making on-site customer visits a regular part of doing business. Each unit on base (squadron level and above) is visited at least once each year. This approach allows customers to communicate any and all C4 requirements they may have directly. These issues are captured and documented in the C4 database for future action. This has significantly reduced the number of requirements and functional downward-directed systems that show up unannounced. A positive working relationship has been fostered between the 35th CS and its customers by being proactive, getting out on their turf, and keeping the lines of communication open.

In the end, the return on investment has skyrocketed while total cost of ownership has been driven into the basement. The 35th CS has made C4 strategic planning a priority. Its efforts have and will continue to pay big dividends for Misawa and the Air Force.

# Hickam's IM warriors: information excellence in all we do

**By Senior Master Sgt. Tom Dikon**
*Supt., Support Flight and 3A0X1 Functional Manager*
*15th Communications Squadron*
*Hickam AFB, Hawaii*

*Photos by Tech. Sgt. Brian Boone, 15th CS*

**Senior Airman John Kim (standing) and Airman Kimberly Clonts analyze monthly data mining metrics to identify improvement areas and reduce postal expenditures.**

If it's "funny how things change," then the evolution of the Information Management (3A0X1) career field over the past few years is nothing short of uproarious. After 21 fantastic years in the information management business – and progressing from clerk typist, to personnelist, to functional manager – I'm convinced our new course is right on target. Nobody demonstrates this better than the IM warriors in the 15th Communications Squadron at Hickam AFB. Here's a team that isn't merely falling in line with future force concepts – they're helping to define this career field's role for the new millennium.

We began our journey in late '97 by taking a hard look at the aftermath of IM's merger into communications – the "ex" IMX troops in SCX, records management and administrative communication teams in SCB, and publishing in the support flight. While the total 3A integration appeared lucrative, it didn't rectify problems which have plagued IMers for years: insufficient cohesion, mentoring and supervision – and especially a void in hands-on, meaningful upgrade and on-the-job training. We were floundering, and there had to be a better way.

We brainstormed, schemed and kicked around a number of reorganization concepts to unite the IM forces, and opted to align all 3A0 positions into the support flight. The FM position in SCX migrated to flight superintendent, and the functional NCOICs and base records manager aligned directly under the FM – the senior 3A0 on base. It provided the necessary IM solidarity and mentoring, which aided 3A and 3C integration, and enhanced IM's critical base support role with heightened visibility. Our critics argued it was nothing more than regressing back to the "ol' base admin days." Don't get me wrong, this alignment would have failed miserably had we not continued to work side-by-side with our networking, infrastructure and help desk counterparts on myriad communications initiatives. We focused on teamwork and processes, not recall rosters. It worked.

Our most innovative development was establishing a "resources and training" element, chartered to initially develop a comprehensive workgroup administration program and provide qualitative upgrade and qualification training to the 3A troops across the base – an overlooked priority for functional IM staffs. We launched our WGA program in January '98 and have since morphed basic CFEPT qualification into an intensive, four-phase workgroup management program that rivals commercial courses costing thousands. The R&T staff now administers island-wide WM training – from desktop applications, to client configuration, to advanced Web and networking concepts, with final certification through network operations apprenticeship, and formal IT certification verified by Dantes. They also manage a unique "comm immersion" program for our staff supporters – full-day indoctrination in all functional areas. R&T also fills an all-too-common abyss in upgrade training and task certification – essential support to our one-deep IM troops and their non-3A super-

visors across the base. Their most recent initiative is writing and publishing a series of on-line CBTs – a cutting-edge crew, dedicated to IM proficiency.

Working in close concert with R&T are the base records management analysts. Base functional area records managers and records custodians receive intensive training in the base IM computer lab, with instruction focused on viable electronic records management processes, video presentations, hands-on exercises, and complete oversight on managing records programs at unit level. ERM principles are incorporated into both WM and RM curriculums, bringing records processes truly "on line" with OPTN concepts, AFI 33-115, Vol I, and the workgroup manager's role. Moreover, once trained, our unit records folks have complete administrative rights over file programs on our local O:/ drive -- our dedicated ERM file server. Training with empowerment -- an awesome combo. RM is also developing a series of local CBTs to enhance the entire spectrum of records management knowledge.

**Tech. Sgt. Mark Seelbaugh (right) conducts an IM mission briefing for Airman Sam Bryant during initial 'comm immersion' orientation.**

The administrative communications and electronic publishing staffs forged ahead with ingenious data mining and automated programs focused on saving scarce dollars and streamlining IM processes. Gone are brown-shoe postal procedures and antiquated manuscript development. Admin comm's data mining analyses save the base thousands a year by controlling mail surges and violations at unit level, while publishing offers one-stop digital tagging and Web posting for newly-approved products. Both agencies provide comprehensive training and dynamic Web sites to educate customers and clients. They round out a pretty high-speed team of information warriors.

Eye-watering achievements at every level, yet their synergistic, collective efforts rival the individual accomplishments. As a team, they've provided the Hawaiian 3A0 community with nearly a dozen island-wide IM forums, numerous RM and WM seminars, Freedom of Information Act, Privacy Act, and activity distribution office site visits and SAVs, and "traveling roadshows" to our joint-service and associate units. The IM team owns base Web policy and drives the annual multi-disciplinary Web site review boards. Factor in thousands of hours of "comm immersion" and in-residence training classes, and you get highly-skilled, informed IM troops at every level of command. Our base IMers also provide all WM and workflow support to the wing battle staff, and made major contributions to the success of JEFX 2000. All, incidentally, while supporting 27 AEF and theater-wide deployments across the globe in the last couple of years.

A tremendous IM cadre, eminently qualified for the many challenges on the horizon. Scarce dollars and competing resources make it tough to secure necessary commercial training, while emerging technologies challenge the way we do business every day. Information managers must be the corps that turns "interim solutions" into enduring workflow processes. Yet as we lean ahead, we must continually address mis-utilization, overcome manning shortages, and remain focused on training, professional development, and mentoring of our future IM leaders.

The 15th Comm IM team makes my job as base functional manager the most rewarding I've ever had. Sometimes it's tough for an "ol' admin clerk" to keep up with today's IM warriors. But not at Hickam -- these guys can "beat the 702" out of anybody.

For more information and downloadable materials, please visit these Web sites:

Records Management:
https://www.hickam.af.mil/CS/LIMITED/SCS/SCSI/SCSIR/

Workgroup Management:
https://www.hickam.af.mil/Cs/Limited/Scs/scsi/scsi/Web/default.htm

Admin Comm Services:
https://www.hickam.af.mil/Cs/Limited/Scs/scsi/SCSIA/default1.htm

Publishing Links:
https://www.hickam.af.mil/Publications/

# Old satellites find new missions

**By Capt. Steven E. Hamilton**
and **Kent E. Chadrick**
*PACAF Computer Systems Squadron*
*and Headquarters PACAF Combat Plans Branch*
*Hickam AFB, Hawaii*

Units in Hawaii, Alaska, Japan and Arizona tested a new concept in voice and data communications while examining the feasibility of using older satellites. This project exemplified Webster's definition of teamwork, involving communications experts from diverse organizations: 293rd Combat Communications Squadron, Hawaii Air National Guard; 3rd Communications Squadron, Elmendorf AFB, Alaska; 612th Air Communications Squadron, Davis-Monthan AFB, Ariz.; Headquarters Pacific Air Forces Communications Directorate; Space Warfare Center, Colorado Springs, Colo.; 18th CS, Kadena AB, Japan; 35th CS, Misawa AB, Japan; and New Skies. These professionals played a special role in the two-day Joint Satellite Communications demonstration of using Incline Orbit Satellites, or IOS.

**What is IOS?**

Most satellites orbit the earth in a geosynchronous and geostationary manner -- they are always in the same spot above the earth every hour of every day. Satellites need fuel to keep their section of space. As satellites get older, fuel conservation becomes important to the controllers, since most commercial satellites own a geostationary "parking spot" in space. If a satellite leaves its virtual box in space, another company could move into the empty slot. So, as satellites get older and lose their ability to maintain their position, companies replace them with newer satellites.

What do you do with a satellite no longer in a stable orbit? Once replaced, many of these old satellites can still send and receive data. As a result, companies move the older satellites to another orbit position and they become Incline Orbit Satellites. An IOS orbits the earth in a geosynchronous manner only -- the north-south orbit restriction is removed (see Figure 1). The satellite under an inclined orbit has greater movement. Maneuvering the satellites in a figure eight pattern conserves fuel and extends the life of the satellite -- up to eight years.

Even though this process extends the satellite's life span, it creates operational issues. Due to their slow change of position within "their spot in space" many earth stations and older ground tactical satellite terminals can't maintain contact. They're unable to keep track of the satellite and need equipment modifications. Another issue is satellite power. With the satellite moving, one should experience power level changes relative to the earth terminal. As a result, the terminal modems require modifications to track the power and keep it at a threshold necessary for effective operations. This modification requires the earth terminal operator to manually program power thresholds.

Although the feasibility of using IOS is not new, the technique and its usage are becoming more viable. Today's warfighter has an increased need for bandwidth. The intelligence, reconnaissance, and surveillance platforms, like Global Hawk and Predator, require significantly more bandwidth than what is available on the Defense Satellite Communications Systems. The expanding network-centric communications, like the Internet and e-mail, have placed an additional demand on bandwidth. As warfighters' bandwidth requirements

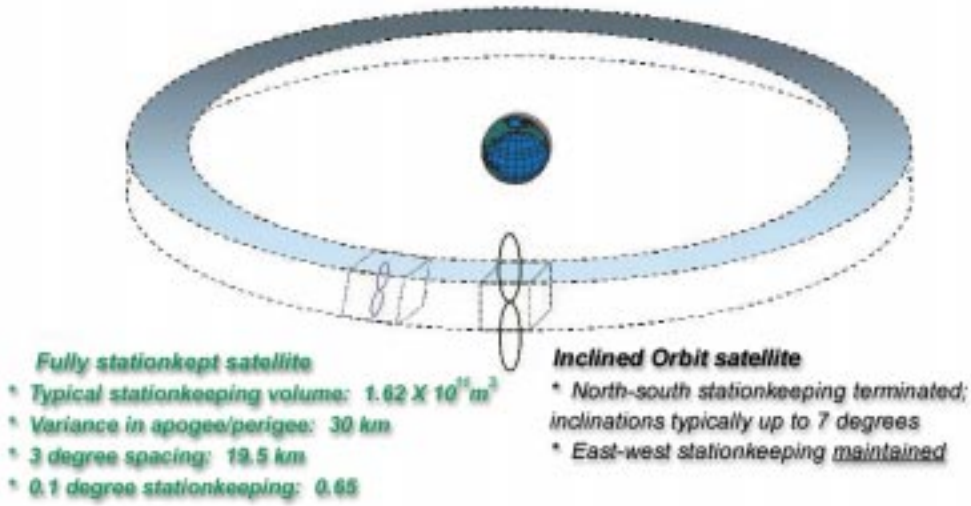



**Figure 1 -- Satellite orbit**

**Figure 2 -- Multiband satellite terminal**

have increased, the Pacific Rim has experienced unique satellite requirements within its area of responsibility. Providing coverage for such a large area and great bodies of water between land masses is a challenge. Commercial frequency band coverage from the Hawaiian Islands to the coast of Asia is practically nonexistent. Enter center stage the possibility of using Incline Orbit Satellites, which provides PACAF a viable solution to support the warfighter. Satellite owners, such as New Skies, have been working hand-in-hand with the Air Force to find a new mission for their older communications satellites.

**The demonstration**

The demonstration was done in January. Locations included: the 293rd ANG unit at Hickam AFB; the 3rd CS at Elmendorf AFB; and the 612th ACOMS at Davis-Monthan AFB. The demonstration was divided into three operational periods and two beam moving (slewing) operations. The first period consisted of the link between Hawaii and Alaska. The SWC captured data and performance characteristics of the Lightweight Multiband Satellite Terminals, which are a part of the new Theater Deployable Communications—and the satellite, while the TDC Initial Communications Access Package performance and necessary configuration requirements were validated (Figure 2). The satellite experienced its greatest movement during this period (Figure 3). Before the second period, we accomplished a beam slewing operation, moving the beam from over Elmendorf AFB to Davis-Monthan AFB. The slewing required only 12 minutes. During the second operational period, data and performance characteristics were documented while the satellite experienced its orbital limits (apogee and perigee). The beam was slewed once again back to Elmendorf, and the final operational period was accomplished. As the demonstration progressed, we improved our processes and performance. The TDC equipment was tested up to its current configuration limit of 4M and the LMST was tested up to the 8M levels. As the satellite slowly moved within its orbit, we were able to see on the spectrum analyzer the terminal modems changing the power levels as needed to keep track of the satellite. Operations were smooth and there was no loss of communications based on the incline orbit characteristics.

**When voice is not voice**

A second objective of the demon-

See **SATELLITES** Page 27

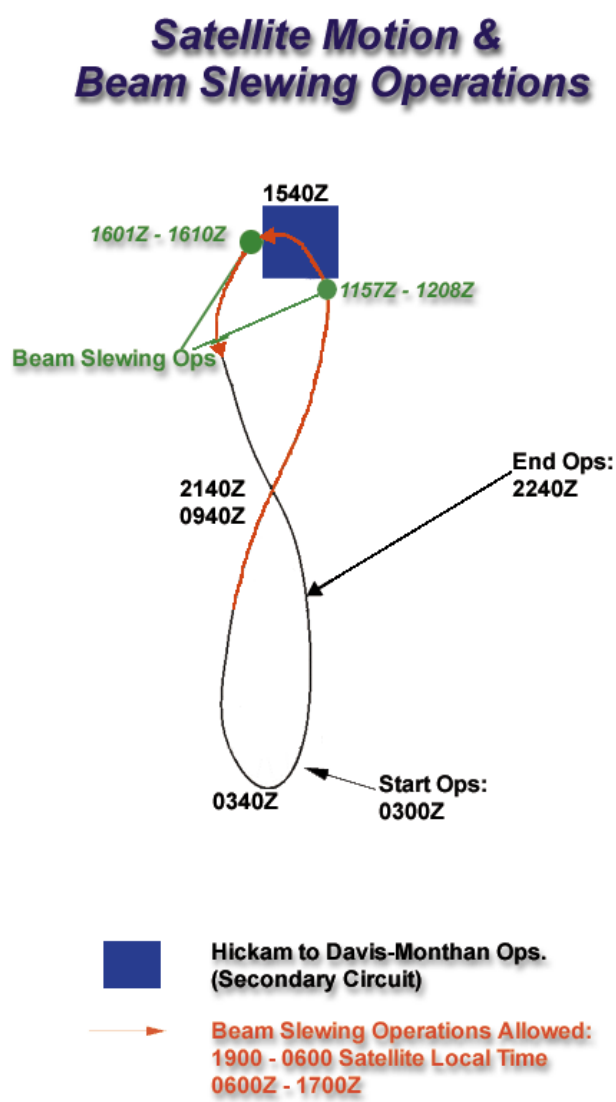



**Figure 3 -- Satellite movement on figure eight**

# 36th CS customers enjoy advantages of Asymmetrical Digital Subscriber Line

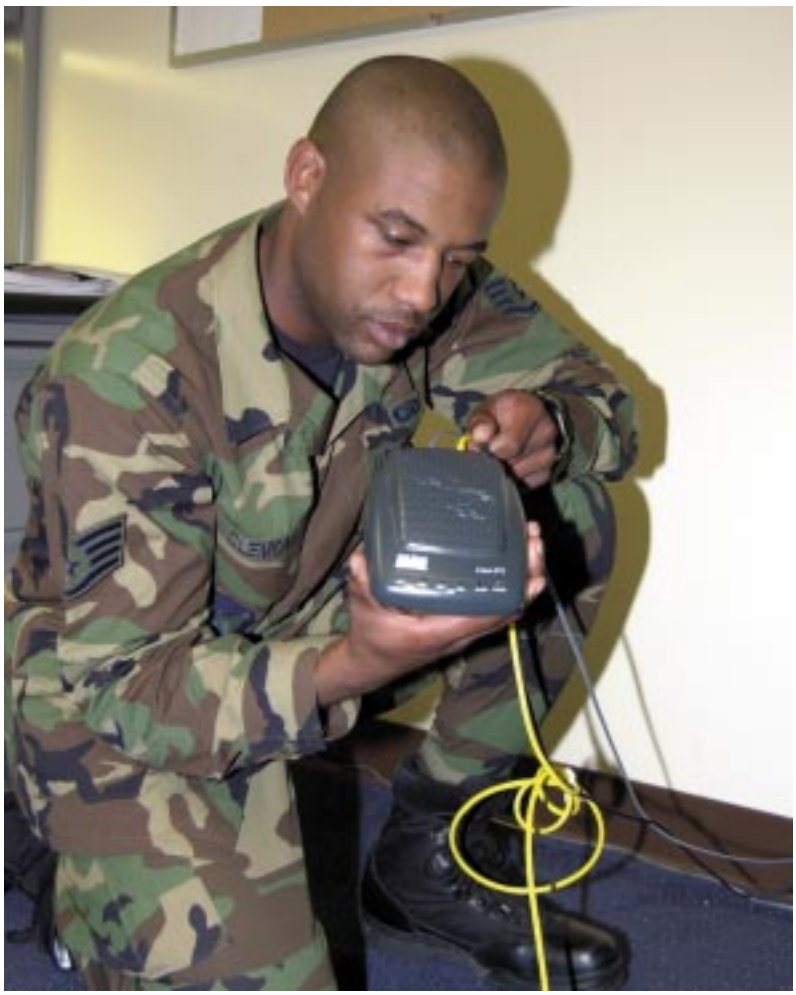
**By Staff Sgt. Barry D. Clemons**
*36th Communications Squadron*
*Andersen AFB, Guam*

Asymmetrical Digital Subscriber Line isn't just a term synonymous with Internet service providers. The 36th Communications Squadron at Andersen AFB has successfully implemented ADSL base-wide. This cutting-edge technology provides rapidly deployable communications services for customers without physical network access.

ADSL has two major advantages. The first is bandwidth. ADSL allows download bandwidth of seven Megabits per second, exceeding the bandwidth of a T-1 connection, which transfers at 1.55 MBit/sec. For the customer, upload bandwidth peaks at 1 MBit/sec.

The second advantage of ADSL is that it's deployed using existing telephone service. This is the biggest advantage for the 36th CS -- no extra cabling and equipment necessary to provide network connectivity to a customer via ADSL.

There are limitless implementations with ADSL. Here at Andersen AFB, the 36th CS provides ADSL to customers in remote locations that either do not have fiber optic cable to their facility, or whose budget would not allow for fiber optic cable to be trenched there.



**Staff Sgt. Barry D. Clemons plugs a cable into an ADSL modem.**

The base's mission is to provide the highest quality peacetime and wartime support to project global power and reach from its vital location in the Pacific. Flight line operations during exercises and contingencies often require network resources to enhance their warfighting capabilities. The cost to install fiber optic cable to every building on the flight line would exceed $500,000. Using ADSL reduces cable installation cost to zero.

The Andersen Visitors' Center has no fiber optic cable and hasn't been able to use the base network. Its location near the front gate would require a fiber-trenching project costing roughly $390,000. With ADSL, connectivity was provided at a fraction of the cost of fiber optic installation.

ADSL has been deployed by the 36th CS to facilities on every corner of the base -- including the base conference center, senior leader quarters, and virtually any location that needs our services.

The cost factor in implementing ADSL far outweighs that of its network connectivity counterpart -- fiber optics. ADSL modems can be purchased at roughly $350 each, and can support up to three network connections with minimal loss of performance. The bandwidth is not regulated as with Internet service providers. Andersen AFB provides the full bandwidth to an ADSL subscriber.

ADSL provides a low-cost, high-speed alternative to normal fiber optic network connectivity. All switched network access points can be replaced with ADSL connections, which saves the Air Force money in installation, equipment and maintenance. The customers' ability to access network resources while using their telephone makes ADSL a dynamic communications solution for Andersen, as well as the U.S. Air Force.

**Voice over IP was one objective of PACAF's demonstration of Incline Orbit Satellites.**

## SATELLITES

*From Page 25*

stration consisted of testing "voice over IP" (VoIP). Typically, voice rides over a circuit which is independent of a data network. For example, when you make a phone call from home, it takes a different path than when you connect to the Internet with your home computer modem -- even though it uses the same lines leaving the house. The reason is voice normally uses a process called circuit switching, where as data uses packet switching. With VoIP, voice is integrated into a data network and treated as data. The VoIP telephone instrument not only has a phone number assigned, but also has an IP address. The instrument along with VoIP networking equipment, converts the voice to data to transverse the network.

For this portion of the demonstration, the VoIP equipment was located at the 293rd CBCS at Hickam AFB and the 3rd CS at Elmendorf AFB. VoIP used the data link established during the New Skies satellite test. The equipment used at each end was a Cisco 3640 router that had special interface cards for commercial phone access, a Cisco 3524 catalyst switch, a server that had the "Call Manager" software and several IP phones that plugged into the Catalyst Switch.

An interface with the TDC/ICAP Redcom voice switch was also tested, which allowed for calls to pass from the analog phones hanging off the Redcom voice switch to the VoIP phones. This proved a call could be made from the classic voice circuit phone to the new voice data phone. So you wouldn't need a VoIP phone to call another VoIP phone.

The demonstration would not have happened without the support of the companies involved. New Skies Satellite Corporation offered its NE 513 satellite and provided the transponder and spot beam slewing time at no cost, and Comtech/EFdata Corporation modified the SLM-8650 modems at no cost, and installed them in the LMST. INTELSAT provided satellite controlling functions and Cisco provided the latest in VoIP equipment.

**Conclusions and the way ahead**

Using IOS has several immediate benefits. Rising demands for satellite airtime have pushed hourly prices through the roof. Inclined satellites, like the one provided by New Skies, offer greatly reduced rates. The current cost of use is more than 50 percent less for traditional satellites. We don't see this benefit changing, especially since the satellites are near the end of their lifecycle. The operational capability of having spot beams slewed to necessary locations minimizes edge footprint degradation. The speed with which beams can be slewed is staggering. Most satellite vendors have short and medium term satellite resources already positioned and scheduled. PACAF considers these benefits to be a win-win situation. VoIP has great potential, especially with its ability to reduce the footprint for initial communications packages by eliminating the need for a voice switch. Using VoIP on a local area network would require only one common data infrastructure.

PACAF's direction is now to coordinate with USSPACECOM and SWC to conduct a formal OT&E on the technique and capability of IOS. The documentation and validation of IOS should help in our support of the warfighter and the increased bandwidth needs – especially of a tactical nature. With the additional bandwidth potential, strategic communications applications can be gained from using IOS. Further still, PACAF supports DISA and its Teleport initiative to upgrade the Standard Tactical Entry Point facilities around the world, and IOS will provide additional resources that can benefit this initiative. In short, to support the warfighter for today and tomorrow, we believe IOS will become a part of the Air Force's future communications backbone infrastructure.

# A day in the life of Wolf Comm can be far from 'typical'

**By Maj. Christina Anderson**
*Plans and Implementation Flight Commander*
*8th Communications Squadron*
*Kunsan AB, Korea*

Anyone who's served in combat communications or a forward deployed location is probably familiar with terms like "Alarm Blue MOPP 4,"and "battle staff directive," and "atropine card." To the 8th Communications Squadron (or Wolf Comm) at Kunsan, these terms represent a way of life. Members of Wolf Comm dedicate themselves to the (Wolf Pack) wing's mission: "Defend the base, accept follow-on forces and take the fight North." As indicated by the following scenario and its special terminology, a day in the life of Wolf Comm can be far from "typical."

Intelligence reports warn of increased enemy activity, with strong indications that Kunsan could be a target of aggression. We immediately put up concertina wire around our buildings for protection against OPFOR (opposition forces). We continue day-to-day activities, but add a review of war plans and THREATCON (threat condition) checklists. The threat increases, and the base implements 24-7 operations.

We immediately break out into day and night 12-hour shifts. Each shift is comprised of a UCC (unit control center) and an alternate UCC, in case something happens to the UCC or its leadership. Critical to the squadron's defense, and its ATSO (ability to survive and operate) during and after conventional and biological attacks, are our sweep teams. Composed of members from each section, the teams man DFPs (defensive fighting positions), defending the compounds and unit leaders, and performing post-attack checks on all facilities for biological agents, UXO (unexploded ordnance) or damage. They also respond to real-world and exercise equipment outages and service interruptions. A large number of comm warriors can be found supporting other base missions as augmentees to security forces, and disaster preparedness and EOD (explosive ordnance disposal) teams.

Wolf Comm and other Wolf Pack warriors hunker down, prepared to prove our mission effectiveness. We accept follow-on forces of the 607th Combat Communications Squadron from Camp Humphreys, who provide tactical communications essential to continued operations should any fixed-base communications facilities be bombed. As the threat increases, we go from Alarm Green MOPP 0 (Mission Oriented Protective Posture 0) to MOPP 2, donning our individual protective equipment. Now, we're under attack…

"Ground attack, all sectors!" We are under mortar or ground attack and immediately take cover. Our troops in the DFPs stay ever vigilant to OPFOR in the area. After the attack, Alarm Black is called, and only the sweep teams can move about the base due to the potential threat of UXO. They report any damage to buildings or equipment to the UCC, which channels the information to the SRC (survival recovery center). The SRC coordinates support from other base units, such as EOD for UXOs, or mobile reserve if we're under attack from small arms fire. Just as we finish our sweeps, and the base is back to Alarm Green MOPP 2 …

"Alarm Blue MOPP 4." We immediately don our gas masks and take cover, praying we haven't been "slimed" with simulated nerve or blister agents. The

*Photo by Staff Sgt. Jerry Morrison*

**Master Sgt. Thomas Guertin, 8th Communications Squadron first sergeant, Kunsan AB, helps build defensive fighting positions that will aid in defending communications assets and people during contingencies.**

**Tech. Sgt. Brian Hosken, 8th CS, radios the unit control center to advise that no unexploded ordnance was found in his sweep area during an exercise.**

*Photo by Staff Sgt. Jerry Morrison*

attack lasts about 30 minutes, but we remain in masks in Alarm Black MOPP 4 until sweep teams can survey the area and give us an all clear. Those not exposed to agents spend almost an hour in their masks before "Alarm Black MOPP 2" indicates they may be removed. But some sweep team members are not so lucky…they must wait a few more hours to be decontaminated before taking off their masks.

In the midst of all these conventional and biological attacks, Wolf Comm must deal with other scenarios – simulated broken limbs, heart attacks, hypothermia and battle fatigue – that test our warriors' self aid and buddy care knowledge and responsiveness. Another exercise input says a commander has become a simulated kill, which tests the ability of others to take on leadership responsibilities. As always, Wolf Comm warriors stay on their toes and prove exemplary in every instance.

Fortunately, we are not in a real war, and all of the scenario inputs described above should have been prefaced with the words, "Exercise! Exercise! Exercise!" But we handle every situation the only way we can – as if it were real. Training for combat is serious business. The Wolf Pack is totally focused on fighting a war from this base, and Wolf Comm plays a huge part in enabling our pilots to "take the fight North." From the post office to the network control center, everyone knows, "No one bombs without comm."

**Capt. Robin L. Mason, Information Systems Flight commander, assigned to the 8th CS, removes concertina wire surrounding the network communications center, after an exercise.**

*Photo by Master Sgt. James Mossman*

# TBMCS unit level working group makes spiral development a reality

**By Capt. Joe Moritz**
*Pacific Air Forces/CSS*
*Hickam AFB, Hawaii*

A problem plaguing software development of military systems is the emphasis on perfecting an entire system before fielding any part of it. This emphasis has caused projects to ultimately fail due to skyrocketing software costs and missed delivery dates associated with attempts to deliver a perfect solution for ever-changing needs of the warfighter. Although attempting to fulfill all requirements before fielding a system is an admirable goal, system developers who follow this paradigm usually leave the warfighter with nothing to execute his mission until the system is completely deployed. To solve this fundamental problem, the Air Force has initiated an evolutionary acquisition process with a spiral development technique as its core feature. This technique was used in developing the Theater Battle Management Core System Unit Level system for the combat air forces, replacing archaic "all or nothing" methodology.

Initially developed as Pacific Air Force's interim replacement for the Wing Command and Control System, TBMCS UL was developed through a team effort of all the PACAF bases with PACAF/DOQ coordinating the efforts. Although it was not formalized, PACAF followed the essence of spiral development by initially fielding a prototype system, receiving inputs from the operational community on how to improve, adding these requirements into the system, and quickly redelivering the improved version to the bases.

The real success was the focus on fulfilling customers' immediate needs by delivering requirements in minimum time. PACAF focused on developing a subset of requirements and quickly delivering the system back to the warfighter for testing. Because PACAF warfighters were so closely involved with the system's development, they had significant buy-in to the system's success. Eventually, the system was accepted as the CAF solution for wing command and control.

Now that CAF has accepted the system, the TBMCS UL working group has formalized system development to follow the spiral development process as outlined in AFI 63-123. To this end, the group has taken the prototype system developed in PACAF and inserted it into the notional prototyping concept. Initial analysis of C2 requirements resulted in a plan calling for an initial series of three spirals, which encompass high level requirements to support the remaining C2 requirements for wartime operation at the wing level. The spiral development integrated spiral development team, or SDIPT, approved a six-month increment fielding and operations for these spirals and the TBMCS UL working group implemented a process for major commands to insert local requirements. As with the original system, the TBMCS UL working group focuses on customer involvement and minimal implementation time to continue to make the project a success.

While requirement definition for future spirals commenced, the current system was inserted into the experiment, operations evaluation, and exercise portions of the concept development process. Led by the 605th Test Squadron, Eglin AFB, Fla., a development test and evaluation and a security test and evaluation were completed at Eglin and a functional development evaluation was completed at Kunsan AB. Results and subsequent derived requirements were provided to the SDIPT for a decision on whether to add the new requirements to future spirals. To reduce spiral development time, the working group combined steps by completing the operations evaluation and exercise sections of the paradigm and the FDE during a base exercise.

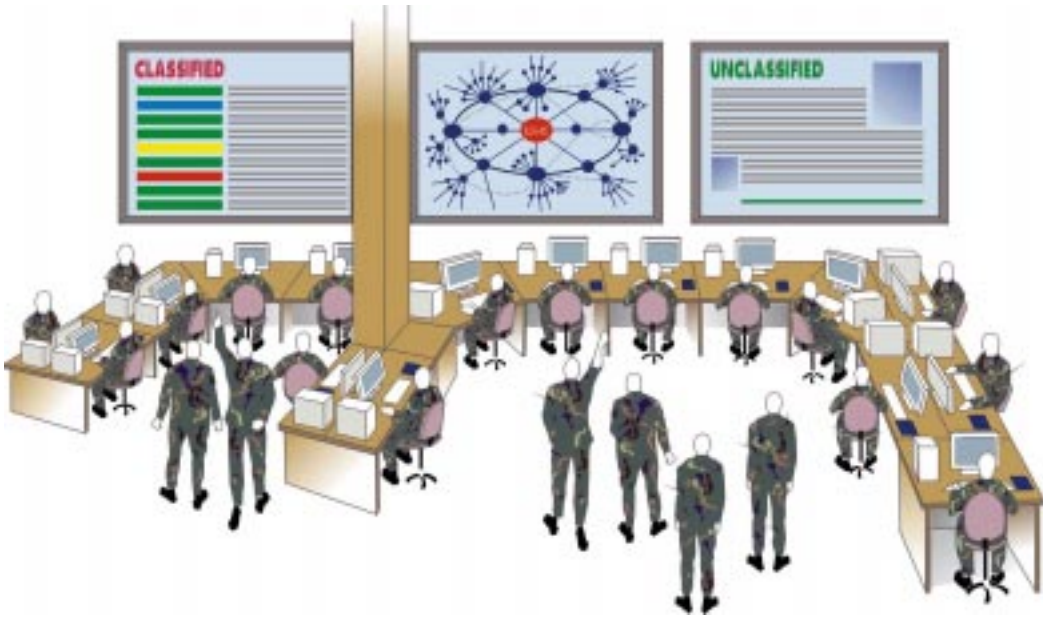
Although this spiraling process has proven successful so far, implementation of this new paradigm has created some issues. During DT&E, for example, there was concern for which requirements the working group should test the system to. This question hits at the center of the paradigm shift, from supplying all requirements in a system to supplying "a core capability meeting valid requirements with the intent to develop and field additional capabilities in successive increments." (AFI 63-123, Page 2) The solution was to test the system against all current requirements. For those that were not implemented, testers noted them as deliverables in future spirals. The fielding decision for this initial core capability was based only on system requirements that were implemented and whether they fulfilled the operators' needs.

The shift from old-school "complete system delivery" to spiral development paradigm has challenged the

See **TBMCS** next page

# Kadena moves closer to realizing 'NCC of the Future' vision

**By Capt. Leonard Giaquinto**
*Kadena AB, Japan*




Air Force manning levels for communications-computer system technicians continue to challenge leadership at bases around the world.

Kadena AB has its share of concerns with manning, especially in the Network Control Center. Network control is housed in two geographically separated buildings. Network management and help desk operations are performed from the main NCC, while information protection, system administration and wide area network duties are performed in the main communications building.

With dwindling resources for desktop computers and computer servers, network professionals tried to find other ways to provide outstanding support to the Kadena warfighters.

"Our personnel are spread out between two facilities, with aging equipment that requires daily intervention from our sharpest technicians," said Senior Master Sgt. Clarence Mathis, the Information Systems Flight superintendent. "We perform our day-to-day mission with about 50 percent of our authorized five-skill levels assigned. We had to find a better way to pool our resources. Our NCC is vital to base personnel who communicate with bases in the United States and the Pacific theater to accomplish their mission."

Maj. Jeffrey Yee, the Information Systems Flight commander, chartered a team of network professionals to identify areas for improvement. Led by Sergeant Mathis, the team focused on consolidating NCC resources.

To cross-utilize communications-computer system technicians across multiple functions within the information systems flight, the 18th CS is fully consolidating all functions within one building.

By consolidating the NCC resources, the flight will optimize the number of personnel required to perform information systems flight operations, while combining unclassified and classified functions under one umbrella. This effort will align the 18th CS with the Air Force "NCC of the Future" vision, that dictates base-level consolidated network operations (AFI 33-115, Volume 2).

The synergistic effects of having all functions within one area will decrease duplication of effort, increase team cohesion, and create more effective on-the-job training opportunities that don't exist when teams are separated.

Although the phased approach is still under development, the flight is making the organizational changes to make the vision a reality.

The project has become one of the squadron's highest priorities as the plans and programs flight has joined the information systems flight in finalizing floor plans, power and air conditioning considerations to meet the objective of the Air Force NCC.

---

## TBMCS

*From previous page*

TBMCS UL working group. However, as the group has further defined low-level activities that relate to spiral development, and worked through questions arising from the paradigm shift, the working group has become more efficient. In the end, the concept has proven invaluable in breaking the chain of continuous requirement definition, in an attempt to perfect a system before deploying it. This new concept keeps the warfighter in the requirements process at each step of development, and allows the developer to quickly get core capability to the wing, so the warfighter can accomplish the mission.

# Giant Voice project amplifies volume

## Outdated system riddled with problems is replaced with one that roars

**By Staff Sgt. Matt Mayou**
*51st Communications Squadron*
*Osan AB, Korea*

Osan's Giant Voice was in whisper mode. Like other Air Force installations worldwide, the facility relied on Giant Voice to quickly convey essential data to all personnel through a base-wide network of speakers similar to a public-address system. It was supposed to relay information on mission-oriented protective posture levels, ground and weather conditions, and any other situation all personnel might need to know about as soon as possible.

Giant Voice was constantly on the fritz, and when technicians went to fix it, they encountered rusty, antiquated equipment and parts. On the cutting edge of technology in 1960, the system had become unreliable and extremely manpower intensive to operate and maintain in 1999. The base received needed help through the combined efforts of base radio maintenance, cable and wire systems, telephone maintenance, antenna maintenance, and the civil engineer.

They began by researching commercial off-the-shelf systems. Base radio maintenance contacted several vendors, and finally selected Whelen Engineering Co. for several reasons. It was the least expensive. It decreased the number of operational zones from 22 to six, vastly reducing required construction and maintenance man-hours. Finally, it was a self-help system that would save the base more than $150,000 for construction and installation, as well as the expense of contracted troubleshooting services.

Their next step was to purchase and install the Whelen system. Within five months, it was installed and ready for testing. Base radio spent a full day putting it through its paces, and were satisfied that it worked well. However, extensive operational testing was required to prove the value and integrity of the system.

During exercise Foal Eagle '99, an accident blew every power amplifier in the system. Base radio had to scramble to get as much of the system as possible operational again. A trip to Seoul to purchase parts solved the problem. Leaders saw how easily this system could fail, and wanted to go back to the old system. However, after continuing to upgrade the system, base radio managed to convince the commander and others that the accident had been a fluke and the system was now much more reliable than the old one.

The final and most insightful upgrade of the system was incorporation of laptop computers and high-tech audio manipulation software. The software (Sonic Foundry Sound Forge XP) saved thousands of dollars by eliminating the need to send integrated chips to Whelen to change onboard messages. Instead, messages were recorded on the laptop, modified as needed, and played back on demand, all at no cost to the Air Force. The addition of laptop computers was not only cost effective, but user friendly. Instead of having to access the Whelen remote console, enter a series of digits and specify the type of alert message he wished to play, the user only had to double click on the appropriate icon, sit back, and watch calmly as everyone reacted, by scrambling into their gas masks or performing other required responses.

The system is also used to broadcast the Korean and American national anthems at the end of each duty day, and "God Bless the U.S.A.," the song popularized by Lee Greenwood, at the end of every exercise. Due to musical limitations of the Whelen system, all of the songs were recorded at Osan with voice only. In fact, the base received so many volunteers that it held a contest to determine who would sing each song. Osan is believed to be the first base to use an *a cappella* version of the national anthem on a daily basis.

In summary, the Whelen system is a huge improvement over its predecessor, in terms of both maintenance costs and performance. The Air Force saved thousands of dollars by using a self-help approach. Although the system nearly floundered in its early stages of operation, base radio restored it rapidly and implemented improvements to prevent further breakdowns and simplify the user interface process.

Through all of its trials and tribulations, the new Osan Giant Voice system has proven to be reliable and steady, and now, instead of whispering, it **roars.**

# Computer help desk provides single-point PC repair for Iceman Team

**By Tech. Sgt. Rica Castro**
*354th Communications Squadron*
*Eielson AFB, Alaska*

Better and faster computer help is only a phone call away, since the 354th Communications Squadron stood up a consolidated help desk. Although a help desk had been at Eielson since 1996, the system hadn't been completely effective.

"Often the technical experts were in other work centers," said Capt. O.J. Dona, 354th CS information systems flight commander. "This typically resulted in less than satisfying results for customers.

"Our old help desk handled more than 45,000 telephone trouble calls and walk-in customers, and more than 500 office visits last year," Captain Dona said. "The workload was dispatched effectively, but not without its problems.

"Customers with basic requests, such as password resets and permission modifications usually got quick service. But anyone requiring extensive individual attention, such as new workstation setups or rebuilds of workstations suffered through long waiting periods. We needed to do something about that," the captain said.

The help desk was swamped with phone calls, while many of

See **ICEMAN** Page 35

**Tech. Sgt. Louis Moussette briefs Col. Cheryl Zadlo, 374th Support Group commander, on how new computers work in the computer learning center.**

# Yokota communicators 'Train to Gain'

**By Tech. Sgt. Louis Moussette**
*374th Communications Squadron*
*Yokota AB, Japan*

"The mission doesn't always allow time to conduct training in the work center." "As soon as I start working on one of the computer based training sets required for duty position qualification, we get called out to complete a job order." These and similar statements are what the 374th Communications Squadron at Yokota AB was hearing from their work center people during the annual training assessment. The commander, Lt. Col. George Hays, said, "The point was clear. A need was identified by the most important people in the training process -- the trainees." Colonel Hays turned to his training manager, Tech. Sgt. Louis A. Moussette, for a solution. The solution was construction of a learning resource center, a 24-hour facility equipped with seven computer terminals providing access to the Internet for CBT, distance education, and formal classes for information management workgroup administrators.

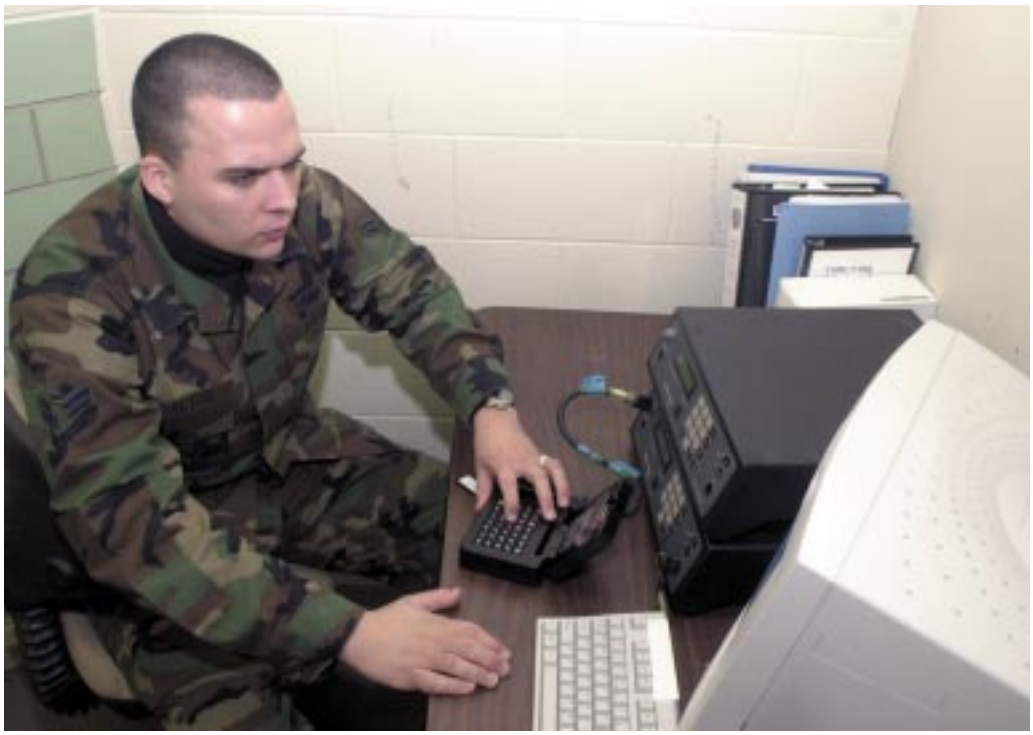
In addition to the upgrade and qualification training, the center is used for formal classes for base workgroup administrators. People need quality training to ensure end users are able to operate computer systems and meet mission requirements. Due to a limited number of trainers, the center makes it easier to provide mission-essential training on new software in a group environment instead of going to each administrator separately. At the same time, workgroup administrators who cannot efficiently use CBT in their office can use the center to complete the certification.

This new learning resource center makes it possible for the largest communications squadron in the Air Force to have an environment where training is a primary focus. The facility provides a place where any member of the unit can get quality training and study job-task knowledge requirements in one of the best environments possible. The center will soon provide airmen in skill level upgrade training pre-testing in preparation for their career development course end-of-course exam. The center operates during normal duty hours on a sign-in basis, unless scheduled training is taking place. After duty hours, airmen who work shifts can access the center by signing out a key with maintenance control. The learning resource center is just one more way to ensure the communicators at Yokota "Train to Gain!"

# Elmendorf leads the way in use of DTD, DMD for cryptographic key management

## Helps save Air Force time and money

**By Monica Barber-Brooks**
*Elmendorf AFB, Alaska*



**Airman 1st Class Aaron Dalton distributes an electronic cryptographic key to a DTD, using LCMS equipment.**

The Elmendorf communications security office leads the way for the Air Force in operational use of the data transfer device, a tool that "puts the cryptographic key in the ignition" of a communications system. Cryptographic keys make it possible to encode and decode classified and sensitive information. They can, for example, permit military aircraft communications systems to send and receive information while rendering it unintelligible to an enemy.

Prior to the advent of DTDs, technicians had to transport paper tapes to each base and physically run them through a reader in order to install a cryptographic key in a system. DTDs represent a quantum leap forward for cryptographic key management.

Using DTDs reduces the human-intelligent threat by taking physical material out of the hands of users. The base reduced the threat by establishing stricter procedures for the main COMSEC account. After an encryption key is transferred from paper tape into the DTD, accuracy is verified, and a backup copy is placed in the main account, the physical copy is immediately destroyed. In July 1998, Elmendorf created local electronic replacement keys for seven base systems. Producing them locally avoided the costs of production at the National Security Agency, shipping via Defense Courier Service, and the manpower required to secure, inventory and destroy physical materials under the old system. The COMSEC office built comprehensive electronic key deployment kits, using DTDs for 3rd Wing aircrews to provide 100 percent of keying material required for exercises and deployments in electronic format. This eliminated the need for 2,700 of the canisters used to transport paper key tapes for communications requirements in Alaska, saving $18,900 annually and reducing the potential for COMSEC incidents.

Elmendorf's COMSEC account was designated lead to implement changes and upgrades in DTD software. The office worked closely with NSA and Science Applications International Corp. to constantly improve software and identify program incompatibilities. The office obtained funds to purchase digital secure telephone equipment units, enabling them to more quickly convert physical COMSEC material to electronic form. It accelerated the process by using the STEs to transfer electronic key information through secure lines to local or globally deployed units. It also developed configuration for defense message system to install more than one messaging client per computer. The COMSEC office was able to meet Alaskan Command requirements with existing resources, saving the government $20,000 in computer acquisitions.

Elmendorf COMSEC personnel inputs were used to write new software for loading unique Alaskan cryptographic equipment vital to early warning systems at Elmendorf and 21 long- and short-range Alaskan ra-

See **DTD** next page

## DTD

*From previous page*

dar sites. The base's reputation for accepting new challenges and leading the Air Force in electronic key usage singled it out as best choice for early implementation and operational testing of the new Fighter Data Link program. A team from SAIC and Headquarters Cryptologic Systems Group gave the office a proposal to implement the FDL system for the F-15 fighter.

FDL is geared to helping pilots fully communicate with one another. The pilot of one aircraft can toggle his display between his aircraft and others flying in the same formation. Wingmen can check each other's armament, fuel load and an array of other parameters. The FDL system significantly improved timeliness for uploading electronic imagery to fighter aircraft. The account's efficiency and the Elmendorf COMSEC team's attention to detail ensure the success rate of FDL flight operations. The system flies virtually every day, surpassing the 80 percent success rate projected in baseline testing.

HQ Pacific Air Forces lauded the management of Elmendorf's base COMSEC account as the "best in command." The migration pace toward total electronic cryptographic key surpasses others in the command. The Elmendorf COMSEC office isn't keeping this information to themselves. They trained 22 people at Kulis ANGB on operation of DTD and helped them implement the Air Force Electronic Key Management System, so they could electronically transfer their information, just as Elmendorf does.

They established procedures to provide emergency COMSEC support to KC-135 squadrons relocated to Elmendorf AFB for five months during runway upgrade at Eielson AFB. This ensured tanker support was available to accomplish air missions in the Alaskan and Pacific theaters. They quickly processed an emergency request for COMSEC keying material from the 962nd AACS while deployed to MacDill AFB, Fla., to support drug interdiction flight operations. In June 2000, the Data Management Device was implemented, allowing Elmendorf to set up a platform to manage its own encryption keys. The DMD also reduced time needed to configure the FDL platform by 98 percent, expediting meeting mission requirements for deployments.

In August 2000, Elmendorf implemented the Air Force Operational General Publication Reporting Environment software. This fully automated system provides accurate information about when COMSEC key material may be destroyed, or if the COMSEC office must maintain it. This eliminates quarterly and semiannual shipments of hard copy documents and publications, annually reducing weight of shipped COMSEC material by 60 pounds and saving $360 in costs.

Just three years ago, cryptographic key material was shipped to Elmendorf on hard copy paper key tapes, and AFKAG publications were only available as hard copy reference books, delivered by the DCS. Today, Elmendorf receives information directly from the NSA Central Facility. Elmendorf can create its own keys for local operational, maintenance and test capabilities, and reduced the number of DTDs the main account requires to meet operational requirements from 77 to five.

Elmendorf fully implemented FDL software at two fighter squadrons, and is preparing to deploy the 19th FS with the first operational use of the DMD at this level.

The Elmendorf COMSEC office leads the Air Force in migrating myriad systems from the work-intensive traditional method to the fully automated Electronic Key Management Systems of the 21st century and beyond.

## ICEMAN

*From Page 33*

the same questions were being asked at job control in the maintenance flight. That duplication led to a solution.

"With the drawing down of U.S. forces worldwide and the similarity between job control and our old help desk, staffing both sections was becoming problematic," said Capt. Sean Murphy, maintenance systems flight commander. "We needed to move smartly and do more with less."

In early December, the help desk and job control combined their functions under the new consolidated help desk.

"This new shop will assist small computer, network and communications maintenance customers," said Master Sgt. John Storm, job control superintendent. "Eielson users can call one shop for help with every comm issue or outage. We can provide the right kind of service for the right kind of outage."

Lt. Col. John Koski, 354th CS commander, explained how the process works. Your call is answered by a consolidated help desk customer service representative. Any problem that can't be immediately resolved is recorded and passed to the appropriate work center. The work center's computer runs a software message system, then sends an immediate pop-up alert notification." Customers receive a work order number to help them track job status.

"Having generalists answer all calls, then directing the job to the expert technicians, speeds our response time," said Senior Airman Benjamin Davis. "The experts have more time to get to the hard problems and work them more quickly."

Captain Dona said the restructuring allows the squadron to serve communications needs more quickly and efficiently.

"With greatly improved network architecture, this setup enhances our Iceman Team mission tremendously," he said.

# Eielson CS welcomes 21st century

**Capt. O.J. Dona**
*354th Communications Squadron*
*Eielson AFB, Alaska*

**Airman 1st Class Brian Crook installs communications equipment in the Eielson AFB control tower.**

Ask anyone who's been stationed at Eielson about the seasons and they'll tell you there are only two: winter and construction. For the 354th Communications Squadron, last summer was one of the busiest on record.

Members of the 354th partnered with Pacific Air Forces and two major communications providers to implement a major upgrade of the base's communications infrastructure. A new storage area network, and clustered file and print servers, will provide a much-needed boost to capacity and capability of the base's metropolitan area network.

Eielson's new project is the first SAN configuration of its kind in the Air Force.

"We needed to build up our communications infrastructure to more efficiently meet the warfighter mission," said Lt. Col. John Koski, 354th CS commander. "Before October, the base network was in terrible shape. Our standard operating procedure was to keep it patched together until our combat information transport system modernization took place. Then we would be able to fix the problems that were so prevalent."

The combat information transport system is an effort to provide a state-of-the-art cabling and network system for every Air Force base in the world.

"We created a half-dozen teams of extremely competent folks and sent them all over the base to upgrade our infrastructure," said Colonel Koski. "CITS brought us to the brink, and we then took the next step and crossed over from 'Band-Aid repair' to a stable network. We called this effort 'CITSKRIEG.'"

The CITSKRIEG cutover took just 11 days, from a legacy piece-meal network, to a fully operational CITS capability featuring an asynchronous transfer mode technology backbone.

The work was well done, according to a technical services representative with a big-picture view.

"We'd been working the transition from the old network to fully using the CITS backbone at Elmendorf AFB for more than a year," said Clayton Brooks, Air Force engineering and technical services representative for both Eielson and Elmendorf. "What was accomplished at Eielson was absolutely stunning, and it's a process that should be modeled for other bases undergoing similar efforts. It was quick. Moreover, it was 100 percent successful.

PACAF systems engineer Jim Corley said this next step in the technology upgrade at Eielson will fix a number of problems left over from the old architecture.

"We need to mitigate problems for the warfighter, including the lack of server space for user programs and personal files, and the inability to perform full backups," Corley explained.

The need for backups was painfully clear to Lt. Col. Fred Guendel, 353rd Combat Training Squadron commander, after a base mail server crashed last year.

"We lost our squadron schedule and had to manually restore hundreds of hours of work," Colonel Guendel said.

The fix was a state-of-the-art storage area network and consolidated server system.

"This is the way to go," said Col. Ronnie Hawkins, Pacific Air Forces director of communications and information. "By consolidating network servers and redirecting cost avoidance into modern storage systems, we provide an enhanced capability for Air Force bases."

The new EMC$^2$ storage area network and Compaq servers provide five new terabytes of storage, and the ability to perform full and partial network-wide backups of all information stored on Eielson. They will also allow users to store information and e-mail files on the network – all this, and the confidence that information will not be lost.

Roger Levy, project director for EMC and lead on Eielson's SAN project, said the networks provide a flexible, change-tolerant infrastructure that can exploit new technology as it emerges.

"We will ensure interoperability and integration with industry-leading technologies," said Levy. "We also assure the training of blue-suiters is a prime focus. Our nation's servicemen and women will not be left in the dark on this technology."

On Feb. 10, the SAN project began processing live e-mail traffic, and by March 1, migration was complete for file servers, print servers and classified data onto a classified SAN.

# Server consolidation is key to *One Air Force … One Network*

**By Capt.**
**John H. Anderson III**
*Base Networks Branch*
*Air Force Deputy Chief of Staff for Communications and Information*
*Washington*

Last summer's Air Force Information Technology Summit laid the groundwork for continued advances in Information Dominance and refined the chief of staff's concept of *One Air Force … One Network*. Three primary initiatives came out of the summit: Design an Air Force portal, establish an Air Force-wide directory, and consolidate e-mail servers. These measures have already yielded results in helping us to work smarter and provide better service at lower costs. Increasing reliability, efficiency, defendability, and manageability and reducing costs – that's a win-win situation for the Air Force and its people.

The initial target was e-mail server consolidation, simply due to the fact that, across the Air Force, there were more than 3,000 e-mail servers. While migrating e-mail servers sounds like a costly and time-consuming process, the Air Force has already made tremendous progress and successfully migrated most of its e-mail services.

On Jan. 3, the scope of consolidation was widened when Air Force Secretary F. Whitten Peters and Chief of Staff Gen. Michael E. Ryan approved new, detailed guidance with three target dates for server consolidation.

Now we're starting to focus efforts on consolidating the rest of our core IT services and functional applications. Core IT services include e-mail, file, print, and network administration and management servers. To date we've identified 4,548 of these servers. Functional applications servers include those for CAMS, JCALS, LOGMOD, FAST, etc. … for which a functional working group has been established to meet the gates of consolidating those servers.

So what exactly is server consolidation? For Air Force servers, it takes on two meanings:

1) Logical consolidation – virtually connecting servers so they appear as one for remote management purposes, and

2) Physical consolidation – actual collocation of servers or even migration from multiple servers to a single server.

The Air Force is doing a combination of both types of consolidation, with a focus on logical consolidation, and performing physical consolidation where it makes sense.

We're making good progress and are postured to see this through. The Air Force Consolidation Plan is being coordinated with the MAJCOMs and Air Staff functional offices at this time. In February we hosted the Server Consolidation Summit and then met with Air Staff functionals and the acquisition community to discuss server consolidation initiatives.

Air Mobility Command is our pilot for server consolidation. Through their efforts, we will solve the technical and operational challenges and validate the proposed solution. They are proving that the outcome is very promising. The first step was standing up a remote administration capability from Scott AFB. They moved one person from each base and installed terminal servers. By doing this, administrators have streamlined their processes to help each other resolve problems. The result has been improved service across AMC. AMC is developing a business case for physically moving their servers to the MAJCOM, with a decision point due in the July 2001 timeframe. As part of the pilot, they have already moved e-mail servers from Charleston AFB (more than 4,800 e-mail users), and are currently migrating McConnell's e-mail servers. Each of these bases gets its e-mail services from Scott AFB, not locally. AMC's next steps are the migration of the other servers from these test bases to Scott, and they are well on their way to meeting the SECAF's gates for completion.

While the "jury is out" on whether it makes good business sense to physically consolidate all servers at the MAJCOM Network Operations and Security Centers, the Combat Information Transport System program is fielding a remote management capability to all MAJCOMs. Air Combat Command is undergoing a field test at this time, with implementation for the rest of the Air Force planned to start in July '01 and be completed by July '02.

Bottom line is … consolidation makes sense: From a corporate position, it allows the Air Force to leverage its IT resources in the continued drive toward Information Dominance. We reduce cost, improve information security, and enable "massing" of experts through consolidation efforts. With continued leaps forward in the way we provide IT services, we will ensure the Air Force realizes the CSAF's vision of *One Air Force … One Network*.

# AFOSI educates members on threats to information systems

**By Col. Eric Patterson**
*Director of Operations*
*Air Force Office of Special Investigations*
*Andrews AFB, Md.*

Air Force Office of Special Investigations is proud to support the Air Force's Information Assurance Awareness Campaign 2001 by helping to educate personnel regarding threats to our information systems and the countermeasures available to combat them. Counterintelligence support to Information Assurance is vital in assuring information is available to our people – and denied to the enemy.

As military operations become more technologically based and reliant on information, traditional means of warfare are becoming increasingly obsolete. As a result, information operations are becoming more vital to the success of the Air Force.

Why is OSI involved in Information Assurance? Because our day-in, day-out involvement in counterintelligence operations keeps you aware of the threats, and AFOSI counterintelligence methods provide the countermeasures to support the Air Force information domain relevant to the warfighter – now and into the future.

Though the Information Assurance campaign is new, OSI's support to Information Assurance has been around for some time. Our program is based on pointing out traditional counterintelligence capabilities as IA countermeasures, in a coordinated fashion to deny or exploit threats to information systems. These traditional countermeasures include our support to "high-risk units" with defensive briefings, technical service investigations to detect and monitor an adversary, computer crime investigations to identify and apprehend network intruders, and establishment of a liaison network enabling quick response and reachback. AFOSI also maintains an aggressive collection and analysis program to put threats into perspective, which ultimately supports investigations and operations to eradicate or exploit operations aimed at Air Force people and systems.

While high-risk units, like network control centers, and network operations and security centers, are a main point of contention, it's important to note that just about everybody these days has a hand in securing our information systems. Realistically, any Air Force person with a networked computer on a desk is a potential weak link in the chain and could cripple our information domain. Only through adherence to sound IA practices, and by teaming with AFOSI to respond with countermeasures, can the chain be strengthened.

# *E-mail solicitation poses new threat*

**By Gina Stokes**
*Counterintelligence Investigations*
*Air Force Office of Special Investigations*
*Andrews AFB, Md.*

*Dear Sir,*

*I am asking you on behalf of a developing nation for your help in obtaining any information you may have access to involving advanced technology and equipment…*

If this message landed in your e-mail inbox, what would you do? Send unclassified information? Forward the message to all your friends? Delete the message and not worry about it?

These are valid questions in the face of a new practice known as "e-mail solicitation." We all know what e-mail is, but what is "solicitation"?

Solicitation is a term used by intelligence agents for the art of conversation, honed by the intelligence professional to its finest edge. It's planned communication, it requires a target, and it presupposes an outcome.

In other words, were an e-mail like the one above to land in your inbox, you should assume it to be the work of an intelligence agent from an adversary, not some innocent plea for information from an unfortunate citizen of an undeveloped nation.

With that understanding of e-mail solicitation, let's get back to the question. What would you do if an e-mail solicitation landed in your inbox?

You might think that deleting it and ignoring the request would be good enough, because the sender would realize you're not interested in providing information and would stop requesting it.

See **E-MAIL** Page 43

# Computer crime investigators engage in war on cyber threats

**By Special Agent Matthew Johnson**
*Computer Investigations and Operations Branch*
*Air Force Office of Special Investigations*
*Andrews AFB, Md.*

The Air Force Office of Special Investigations fields a team of 48 specially trained agents to ward off hackers, thwart computer criminals, and detect cyber terrorists.

They're called computer crime investigators, or CCIs, and escalating threats from the cyber world keep them on their toes. Probes and scans of Air Force computers from foreign locations alone number in the millions per year.

The need for vigilance against such threats is clearly demonstrated by the damage caused to the Air Force by last year's "I Love You" computer virus:

* Number of users executing the virus: 7,418
* Number of servers offline: 1,065
* Average downtime: 32 hours
* Total cost: $3,174,427

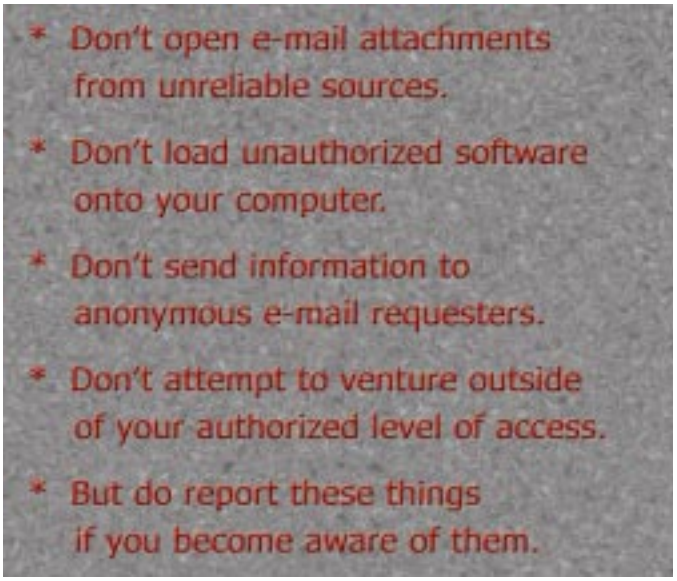
Imagine such a crippling attack – or several at one time – during wartime operations, and it's easy to understand why Information Assurance is so critical to the Air Force.

It's also easy to understand why so many adversaries choose to operate in cyberspace: Their attacks are harder to identify, they benefit from the rapidity of information flow, they can inflict great damage without great expenditure, and cyberspace provides a virtual sanctuary from identification.

And that's why CCIs have become increasingly important. CCIs provide rapid response to intrusions into Air Force information systems and networks worldwide. These officer, enlisted, and civilian agents are dispersed to seven primary locations around the world, supporting OSI field units and Air Force commanders in their respective areas of responsibility.

CCIs provide threat information, analysis, operations and intelligence support by engaging investigations and Information Assurance issues with military and civilian Computer Emergency Response Teams, other military and federal law enforcement entities, and intelligence agencies.

In addition to providing response to high profile viruses, CCI's primary caseload revolves around traditional computer intrusion investigations. In 2000, CCIs opened 26 substantive computer intrusion investigations. Half of these originated in foreign locations.




Intrusions that originate from the United States are broken down into two categories: traditional intrusions and intrusions from "insiders."

Insiders are Air Force members, employees or contractors with access to Air Force information or systems who exceed their authorized access. Because of their regular access to information systems, insiders present the greatest potential for causing harm. (See related article on Page 41.)

While CCIs are critical to the war on cyber threats, they can't do it alone. They depend on every Air Force member complying with sound computer practices. Don't open e-mail attachments from unreliable sources. Don't load unauthorized software onto your computer. Don't send information to anonymous e-mail requesters. Don't attempt to venture outside of your authorized level of access. But do report these things if you become aware of them.

If you see a violation or exploitation of an Air Force resource or information system, immediately notify your assigned security officer or local OSI detachment. You may just foil the attempt of an adversary who seeks to harm our information systems.

CCIs of the Air Force Office of Special Investigations remain postured to respond effectively and rapidly to threats against our information systems and infrastructure. Their capabilities, coupled with your help, can combat some of our most advanced adversaries and ensure our members operate in the safest environment possible.

# AFOSI and AFMC team up to provide unique approach to IA

**By Special Agent Zachary Smith**
*Air Force Office of Special Investigations*
*Region 1*
*Wright-Patterson AFB, Ohio*

*Photo by Master Sgt. Timothy S. Polk, AFMC NOSC*

**Standing from left: Special Agent Kenneth C. Koch, SA Henri M. VanGoethem (OSI Computer Crimes Investigations and Operations), Lea Culver (CACI, AFMC NOSC contractor lead), and (sitting) David E. Bone (Aegis Research Corp IA Analyst and Investigator).**

Since December 1999, Air Force Office of Special Investigations Region 1 and Air Force Materiel Command have engaged in a mutually beneficial collaboration for defensive counterinformation and Information Assurance efforts. AFOSI assigned contract information operations analysts to the AFMC Network Operation and Security Center within an overall concept of operations to protect Air Force intellectual capital on AFMC networks.

This is the first such collaboration in the Air Force, and it's been prompted by the need to protect the command's science and technology capital. This critical resource that resides on AFMC's information infrastructure is uniquely developed, held and shared in a culture emphasizing openness and beneficial technology transfer. It links to AFMC and Air Force S&T protection requirements, primarily through the Air Force Research Laboratory and AFMC Director of Requirements.

This partnership directly supports AFMC DCI, network enterprise management, network situational awareness, and overall IA efforts. The goal is to prevent intrusions, identify potential threats to network integrity, and offer an extra layer of protection to critical research networks. It provides proactive threat-based analysis that enhances network security countermeasures by identifying information at risk, and previously undetected exploitation protocols, and by raising awareness in the information owner.

The level of activity monitored by IO analysts and NOSC operators is lower than what is monitored by the Air Force Computer Emergency Response Team, and is focused at AFMC locations, with special emphasis on AFRL sites. In addition to developing new technologies, weapons and applications, AFRL is a key source of authorized technology transfer in the Air Force. It relies on the availability and security of the Defense Research Engineering Network to conduct research without losing it to non-authorized foreign elements. That is what makes this initiative notable: It integrates several elements across AFMC to enhance IA and protect critical technology over the entire research and development, and acquisition lifecycle. During contingencies, additional consideration is given to certain AFMC information systems, such as air logistics centers, which are crucial elements in global reach and power, and unique to AFMC.

The AFMC NOSC and AFOSI exploit data to identify criminal and intelligence indicators to detect and deter activities that threaten the security of AFMC networks. They fuse additional information, shifting to a proactive approach (vice intrusion response) by placing emphasis on the intent of those who threaten the networks. This collaboration involves computer crime investigators who develop hostile profiling and investigative opportunities to mitigate the threats and get in front of crime affecting AFMC systems.

The ability to tailor analytic support to the direct needs of the Air Force S&T community at the point of requirements generation distinguishes this from other MAJCOM programs. Linkage to other threat indicators drives time sensitive threat countermeasures to protect technology at risk. This may involve enterprise configuration management, or other actions taken to prevent network and information compromise.

As the Internet expands worldwide at an explosive rate, Air Force networks face an increasing security threat. AFOSI and AFMC have teamed their capabilities to mitigate this threat to AFMC, AFRL and tenant networks, remaining vigilant to would-be intruders, and increasing the awareness of commanders and users to the information threat.

# *Insider poses greatest potential threat to Information Assurance*

**By Special Agent Chris Mariano**
*Information Operations Branch*
*Air Force Office of Special Investigations*
*Andrews AFB, Md.*

Who's the greatest potential threat to Information Assurance?

The insider.

Anyone who has authorized access – either physical or electronic – to information and infrastructure resources, is an insider, and it's the insider who's in the strongest position to cause harm to our information systems.

Throughout history, significant problems have been created by insiders, whether acting as agents of an enemy government or simply being disgruntled employees with an ax to grind. In any case, their authorized access to information, the trust placed in them by their superiors, and their first-hand knowledge of asset value lend particular gravity to the damage they can do.

Never has this been more true. Why? Because in today's high-tech workplace, enormous processing power and interconnected information systems have become commonly available. This enables the insider to access, correlate and associate more information from a greater number of information sources than ever before.

Insiders have the capability to disrupt interconnected information systems, to deny the use of information systems and data by other insiders, and to remove, alter or destroy information. Even worse, aided by sophisticated and well-resourced outsiders, the severity of insider malicious activity may be significantly amplified.

Making matters worse, insider misuse is harder to detect because it can operate at a higher semantic level than penetration by an outsider masquerading as an insider. Moreover, outsiders can quickly attain many characteristics of an insider, making them difficult to discover.

Insider threats are posed equally to closed systems that process classified information and to open systems that process unclassified information. Each is vulnerable to malicious insider action. After all, closed systems employ the same commercial off-the-shelf software and hardware components used for open systems. The only difference, really, is the physical security, unique communications protocols, and encryption that protects communications paths and prevents interception or disruption among network components.

What this means is an insider with malicious intent can cripple a closed system as effectively and quickly as an external expert can cripple an open system. In fact, the insider may have an easier time of it, due to his or her knowledge of the system and its controls, and the fact he or she is usually under no particular suspicion.

Insider security problems arise primarily from four attitudes:

* **Maliciousness:** the deliberate compromise or destruction of information, or disruption of services to others.

* **Disdain for security practices:** the willful public display of classified information, improper storage of classified materials, improper destruction of classified or unclassified data, or the inadequate protection of classified material outside of controlled facilities.

* **Carelessness:** any act of disregard to the proper use of an information system or the protection of information, not necessarily meant to exploit, attack or otherwise adversely affect information systems.

* **Ignorance:** lack of knowledge of security policy and practices to prevent the compromise of information.

Needless to say, an insider – especially one with malicious intent – can compromise our military effectiveness and place in jeopardy the lives of our military men and women.

Because of all of this, an Insider Threat Integrated Process Team was mandated by the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The team was chartered "to foster the effective development of interdependent technical and procedural safeguards" to reduce malicious behavior by insiders.

No nation has ever been able to eliminate the insider threat. The challenge is to continuously assess the threat, reduce our vulnerabilities, and seek new countermeasures.

# Make sure you're not 'bugged'

**By Special Agent David A. Gollem**
*Air Force Office of Special Investigations Det. 502*
*Ramstein AB, Germany*

Not all bugs bite. Some just listen.

This kind of bug is the type that a spy tries to plant in your work environment to eavesdrop on conversations and transmit sensitive data to the enemy.

Making sure you're not "bugged" is always important, but it's particularly difficult in a deployed environment, where facilities are frequently temporary structures. To make matters worse, deployed locations are typically "tips of the spear" fighting units, with much classified information coming in and going out.

For this reason, people serving in deployed locations need to be particularly careful to take the necessary steps to prevent bugs.

Most important is the need to establish positive physical control over all areas where classified or sensitive information is discussed, handled or processed. Remember, the objective is to deny spies the ability to enter, install a listening device, and leave without your knowledge.

Ensure that all windows, doors and locks are under your direct control. High-security locks should be used whenever possible, and rekeying them may be required from time to time.

However, because the installation of good locks is not always an option in deployed locations, the use of tamper-proof seals, along with a continuous inspection of the seals, may be useful. Also, keep in mind that cipher locks shouldn't be considered adequate for physical security. They're OK for controlling access to certain areas, but they're too easily bypassed to be relied upon for physical security.

Instead, establish positive physical control – in the form of an entry control point, preferably at one location – over the areas that discuss, process or handle classified and sensitive information. Ensure the facility can be secured to the appropriate level for the information being protected.

If relying on 24-hour manning to secure an area, the people inside must be able to immediately detect unauthorized access to any part of the facility. This is important because a good bug need not always be placed directly inside the target area. Often an adjoining area will work just as well.

The proper escort of visitors is also crucial. Escorts should vigilantly watch visitors, not only to ensure they don't take anything they're not supposed to, but also to ensure they don't leave anything "extra" behind.

Believe it or not, good housekeeping also plays a role. Ensure only mission-related materials are kept in the area. This is important because many bugs are hidden in "Trojan horses." If you don't know what you have, how will you know if something "extra" has been added? Garbage and cluttered areas provide excellent camouflage or hiding places for bugs. Along those lines, identify, inventory, and control all items in your area.

Speaking of clutter, can you identify all the cables and electrical cords tangled up beneath your desk? Cluttered and unidentified cables and wires provide superb camouflage for bugs. Unused cables provide a ready-made communications path in and out of your area.

Therefore, identify every cable entering and exiting your area, and route all electrical and communications wiring through a minimum of centralized egress points.

Remember, too, that sound can carry a long way. Soundproofing or other audio attenuation may be required. Be on guard for open windows, gaps under and around doors, and walls that are common to areas occupied by uncleared personnel.

Finally, consider requesting a Technical Surveillance Countermeasures survey. This is a counterintelligence investigation conducted by the Air Force Office of Special Investigations, Army Military Intelligence, or the Naval Criminal Investigative Service. The survey employs specially trained agents and equipment to determine if your area has been bugged, either with a listening device or by a video or computer device.

A TSCM survey, conducted at the appropriate time, is an integral part of information protection. Consider requesting one as soon as you have moved in all furnishings, all equipment is installed and operational, and you have taken control of and secured your area.

The availability of TSCM survey teams is limited, and their services are costly. Therefore, they are prioritized on the basis of sensitivity of the information being protected, not by the rank or status of the person requesting the survey.

For more information, contact your servicing detachment of the Air Force Office of Special Investigations.

**Establish an entry control point.**

# Threats to IA on the rise

**By Special Agent Daniel Fleeger**
*Headquarters Air Force*
*Office of Special Investigations*
*Andrews AFB, Md.*

As our reliance on computers and information systems has grown, so has our adversaries' propensity for exploiting them to do damage.

The Air Force has experienced a steady increase in the number of attacks against its information systems, and experts agree that the number of attacks is only going to increase.

One reason is the availability, ease of use, and sophistication of publicly available computer-attack software. Such attacks once required the skills of a computer expert. They can now be achieved by the novice computer user armed with easily obtained software.

The novice attacker is not the only threat. In general terms, computer and information systems attackers can be grouped into five major categories.

* The foreign intelligence service operative is an aggressive adversary who attempts to exploit our information infrastructure for intelligence purposes. He or she can identify our members, evaluate their level of access to information of intelligence value, and even recruit their services … all in cyberspace. There are significant advantages to doing business this way, such as easily concealing one's identity, the rapidity of information flow, and plausible deniability.

* The cyberterrorist attack goes beyond mere computer intrusions, denials of service or defacing of Web pages to actual destruction of data or systems. Use of the Internet and other information systems gives terrorist groups a global and near real-time command and control communications capability. Because such groups have limited resources – and electronic intrusion can help them achieve their objectives at minimal cost – it's expected that cyberterrorism will increase.

* Organized crime targets computer systems to commit fraud, acquire and exploit proprietary information, and steal funds. Criminal organizations use electronic intrusion to hinder police investigations, collect intelligence, destroy or alter data on investigations, and monitor the activities of informants.

* Hackers, not too many years ago, were motivated primarily by curiosity about computer systems and network operations. In most cases, they were unlikely to engage in serious criminal activities. In contrast, today's hackers appear to be motivated by greed, revenge and politics, and their actions have become more malicious. They are more likely to aim their attacks not just at individuals, but also at enterprise information systems.

* The malicious insider, who has legitimate access to proprietary information and mission-critical systems, poses a significant threat because of having trusted status and familiarity with security practices. When an insider betrays his trust, he has a much greater opportunity and ability to do harm than anyone on the outside. Moreover, he is less likely to be detected. The malicious insider, motivated by greed, revenge, or even political ideology, can act alone or with outsiders.

As you can see, the threats to Air Force information systems are numerous and significant. To combat them, the Air Force Office of Special Investigations brings to bear a number of capabilities, including defensive briefings to high-risk units and personnel, countermeasures against technical surveillance devices (or "bugs"), computer crime investigators who specialize in combating crimes against computers and information systems, and counterintelligence investigations.

But OSI can't do it alone. Everyone with access to computers and information systems is a partner in the war against cyber threats. If you detect intrusion activity, or receive unsolicited or suspicious e-mail, or discover new software or tools on your computer, or witness unescorted visitors in your work area, you should immediately contact your security manager or the local OSI detachment.

Familiarize yourself with the signs that an insider might be up to no good. Be wary of an insider who shows a keen interest in hacking techniques and system vulnerabilities. Take note if an insider has configured his or her computer to provide capabilities that it shouldn't have. Other traditional indicators may be observable too, such as unexplained affluence, abnormal requests for information, and a propensity for security violations.

**E-MAIL**
*From Page 38*

Besides, even if the e-mail did come from overseas, reading it wouldn't be considered an actual foreign "contact," so there would be no need to report it. Right?

Wrong!

"Contact," in this context, means any exchange of information directed to an individual, including solicited or unsolicited telephone calls, e-mail, radio contact, and so on, in addition to face-to-face meetings.

Therefore, receiving an e-mail solicitation is a reportable incident, and the provisions of Air Force Instruction 71-101V4(2.7) require it to be reported to the Air Force Office of Special Investigations within 30 days, either verbally or in writing. If the recipient doesn't have access to the OSI, then he or she can report it to his or her commander, supervisor or security officer, who then must provide the information to the servicing OSI detachment.

A good rule of thumb is to report any unusual activity. It's better to be too cautious than not cautious enough.

For more information, contact your local OSI detachment.

# Air Force names Maintenance Effectiveness award winners

The Air Force has announced its maintenance effectiveness award winners for 2000. The maintenance effectiveness award recognizes units that have best managed their resources with criteria based on unit accomplishments, effective use of maintenance resources, innovative management actions, and quality of life programs.

Winners of the 2000 Air Force maintenance effectiveness awards include the following:

Communications-Electronics (Large) — 86th Communications Squadron, Ramstein AB, Germany

Communications-Electronics (Medium) — Det. 1, USAFE Computer Systems Squadron, Kapaun Air Station, USAFE

Communications-Electronics (Small) — 437th Communications Squadron Charleston AFB, S.C.

Additionally, the 86th Communications Squadron was selected to compete for the DOD maintenance awards and Secretary of Defense Phoenix Trophy in the small unit category.

# Comm and Info officers nominated for promotion

**General Croom**

Two communications and information officers were nominated by the President to the Senate for promotion to major general. They are:

Charles E. Croom Jr., vice director, J-6; and deputy director for defense-wide Command, Control, Communications and Computer Support, J-6 Joint Staff, Washington.

**General Meyerrose**

Dale W. Meyerrose, director, Command Control Systems, J-6, Headquarters North American Aerospace Defense Command and Headquarters United States Space Command; and director, Communications and Information, Headquarters Air Force Space Command, Peterson AFB, Colo.

**Colonel Lord**

Another communications and information officer has been nominated by the President to the Senate for promotion to brigadier general. The nominee is William T. Lord, director, Communications and Information, Headquarters Air Mobility Command, Scott AFB, Ill.

# AF announces Lt. Gen. Leo Marquez award recipients

The Lt. Gen. Leo Marquez Awards are presented to communications-electronics maintainers who have demonstrated the highest degree of sustained job performance, efficiency, knowledge and results, and direct involvement in sortie generation. General Marquez retired from the Air Force in 1987 as deputy chief of staff, Logistics and Engineering, Headquarters U.S. Air Force. Throughout his career, General Marquez held front line maintainers in the highest esteem. He believed they were the key to mission accomplishment.

The winners for 2000 are:

Communications-Electronics Maintenance Field Grade Manager – Lt. Col. Linda R. Medler, Dover AFB, Del.

AMC Company Grade Manager – 1st Lt. Tristan Morel L'Horset, Ramstein AB, Germany, United States Air Forces in Europe

Supervisor Manager – Senior Master Sgt. Jeffrey P. Johnson, RAF Mildenhall, England, Air Force Special Operations Command

Technician Supervisor – Staff Sgt. Richard A. King, Ramstein AB, USAFE

Technician – Senior Airman Jennifer L. Hochstedler, RAF Mildenhall, AFSOC

Civilian Manager – Michael C. Williams, RAF Croughton, England, USAFE

Civilian Technician – Gerald R. Snodgrass, Malmstrom AFB, Mont., Air Force Space Command

Each military member selected is authorized to wear the Air Force Recognition Ribbon. Civilian employees selected may wear the Air Force recognition lapel button.

# Comm and Info Hall of Fame dedicated at Scott

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

*Photo by Master Sgt. Ed Ferguson*

**Lt. Gen. John L. Woodward Jr. (right), Air Force deputy chief of staff for Communications and Information, and Col. Thomas J. Verbeck, Air Force Communications Agency commander, cut the ribbon at the Comm and Info Hall of Fame dedication ceremony.**

"As we enter a new millennium with all the challenges and opportunities it holds, it's important we remember those who came before us and laid a solid foundation for today's Air Force communications and information professionals," said Lt. Gen. John L. Woodward Jr., Air Force deputy chief of staff for Communications and Information. During a visit to Scott March 2, the general took time to pay tribute to former communicators for their lasting contributions to the communications and information business by dedicating the Communications and Information Hall of Fame in Building 1700, the Lt. Gen. Harold Grant Building.

In 1999, the Air Force established the Hall of Fame to honor and remember individuals who made significant contributions to the Air Force and the communications and information career field while serving in the public and private sectors.

The names and photographs of the inductees are permanently displayed.

The Hall of Fame includes 20th Century "Foundation Setters". Brig. Gen. Billy Mitchell, Gen. Edwin Rawlings, Lt. Gen. Harold Grant, Lt. Gen. Lee Paschall, Maj. Gen. Harold McClelland, and Maj. Gen. Robert Sadler are recognized for their pioneering leadership and unselfish dedication to the nation. "They created a lasting groundwork for our community to build on through the 21st century," said General Woodward.

Last year General Woodward announced the Communications and Information Hall of Fame "Class of 2000" at the Retired General Officers Conference at Andrews AFB, Md.

"These visionaries guided the Air Force toward a technological and information-enabled future and began the tradition of excellence," he said.

They include Lt. Gen. Winston D. Powers, Maj. Gen. Robert L. Edge, Brig. Gen. Ivan L. Farman, and Col. Glenn Giddings. The first inductee in 1999 was Lt. Gen. Lee Paschall.

"It is an honor and pleasure to dedicate this Hall of Fame today and recognize these distinguished founders and communications and information leaders," said General Woodward.

"These pillars of strength are our 20th century communications legends. They left an enduring legacy and paved the way to information superiority for our Air Force," he said. "The Hall of Fame recognizes an elite list of individuals who helped ensure the Air Force has the best communications and information capabilities in the world."

The Hall of Fame inductees are featured at the AFCA Web site: http://public.afca.scott.af.mil/public/fame/

The Communications and Information Foundation Setters are featured in a video available at the Defense Automated Visual Information System/Defense Instructional Technology Information System site. The PIN record— Production Identification #613976—is for online ordering of the product through the Defense Visual Information Web site at: http://dodimagery.afis.osd.mil/dodimagery/davis

# Next generation cell phones may impact AF operations

**By Nelson Pollock**
*Air Force Frequency Management Agency*
*Washington*

The frequency band used by Air Force precision guided weapons flown against Iraqi targets may be auctioned off in the United States to the next generation of public cell phones – also referred to as Third Generation, or International Mobile Telecommunications – 2000.

Last May, an international spectrum conference identified several frequency bands to study for potential IMT-2000 use, including the one used by the Air Force's GBU-15 precision guided weapon.

Soon after the conference, the president issued a memorandum that directed executive branch agencies to work with the Federal Communications Commission and the commercial sector to select by summer 2001 a frequency band the FCC can auction to satisfy increased demand for IMT-2000 radio frequency spectrum access. One frequency band under consideration is allocated on an exclusive basis to the federal government (1755 - 1850 MHz) and supports many critical Air Force and Department of Defense functions. Another frequency band under consideration is allocated on an exclusive basis to the civil sector (2500 - 2690 MHz) and is used for high speed wireless broadband services, such as sending instructional TV to public schools.

TV and print ads abound regarding the new services available for cell phones. Soon users will be able to hold in their hands devices that provide wideband Internet access and full motion video conferencing – and they'll be able to do it in any country.

However, providing these additional services comes at a price: increased demand for bandwidth.

Lately Congress has used reallocation and auctioning of federal government spectrum to provide the additional bandwidth for new civil telecommunications applications. Naturally everyone would like to take advantage of new technologies – both as Air Force personnel and members of the public.

As a result of the Presidential Memorandum, federal agencies were required to provide the National Telecommunications and Information Administration, the president's spectrum manager, with documentation on the technical, cost and operational impacts of possible public use of the 1755 - 1850 MHz frequency band. The FCC led a similar effort to describe and quantify the civil sector's use of the 2500 MHz band, also under study for U.S. implementation of IMT-2000.

The goal of the national IMT-2000 study is to provide detailed information upon which to base a spectrum selection by July of this year. The identified spectrum will be auctioned by September 2002.

The auction value of spectrum can be enormous. A recent FCC spectrum auction for about 40 MHz yielded more than $16 billion, or about $425 million per MHz. At that rate, the auction value of a single Air Force air traffic control radar frequency assignment would be about $2 billion!

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence tasked the Defense Information Systems Agency's Office of Spectrum Analysis and Management to coordinate the DOD input to the national IMT-2000 study called for in the president's memorandum.

The interim federal (including DOD's input) and civil IMT-2000 study reports, and other Third Generation information are posted on the NTIA Web site at URL: http://www.ntia.doc.gov/osmhome/reports/imt2000/.

On Feb. 9, DOD provided a copy of its final IMT-2000 report on schedule to NTIA. The report documents our use of the 1755-1850 MHz frequency band and analyzes the cost and operational impacts of three scenarios for possible accommodation of IMT-2000 in that spectrum, including military and civil sharing of the entire band, sharing of portions of the band, and DOD vacating the band to another spectrum suggested by NTIA.

The NTIA and DOD final reports were scheduled to be posted on the Web by this month.

The Air Force Deputy Chief of Staff for Communications and Information tasked the Air Force Frequency Management Agency to lead the Air Force portion of the DOD IMT-2000 study. AFFMA engaged many other Air Staff and major command organizations and System Program Offices in the effort. For example, the Air Force Cost Analysis Agency developed costing data for various sharing scenarios. Air Force Space and Missile Systems Center and Air Force Space Command developed the cost, technical and operational impacts for the Air Force Satellite Control Network and military satellite receivers. Similar data on Air Force terrestrial systems came from the Precision Strike and Air Combat Training SPOs at Eglin AFB, Fla. In addition to AF/SC, key participating Air Staff directorates included the executive officer, comptroller, maintenance and acquisition.

The Air Force uses the 1755 MHz frequency band for many mission critical functions, such as military

See **PHONES** next page

## PHONES

*From previous page*

satellite uplinks, precision guided weapons, air combat training systems, and base and range infrastructure links.

The other military departments have participated in the DOD IMT-2000 study and national IMT-2000 discussions. For example, the U.S. Army's Mobile Subscriber equipment and U.S. Navy's Tactical Air Combat Training System also operate in the 1755 - 1850 MHz band.

In addition, the OSD is very involved in this issue. The DOD Office of General Counsel is coordinating with the MILDEP and DISA General Counsel offices to provide legal and strategic policy inputs to the overall DOD IMT-2000 strategy. The OSD Cost Analysis and Information Group chaired the DOD IMT-2000 Costing Working Group and provided excellent review and inputs on the financial impacts of any reallocation of the band.

The official DOD input to NTIA's IMT-2000 report, recently signed out by the deputy secretary of defense, concluded that IMT-2000 and DOD systems could not share a spectrum at the same time. The report also documented the technical, financial and operational impacts of moving systems totally or partially out of the band.

Civil federal agencies within the executive branch are also very concerned about the possible reallocation of this federal spectrum to public and commercial use. For example, the FBI operates many law enforcement and public safety telecommunications links in this spectrum. The Departments of Energy and Agriculture depend on this spectrum for sending a variety of data over fixed point-to-point links.

The FCC, with private sector input, is preparing a similar study regarding possible accommodation of IMT-2000 in the public and commercial 2500 MHz frequency band currently used for educational TV and broadband wireless systems.

Over the next few months the Air Force will be working closely with OSD, the other military departments and defense agencies, NTIA, FCC and others on the final selection of IMT-2000 spectrum in the U.S.

Under current U.S. law, the FCC can not reallocate federal spectrum without the concurrence of the executive branch.

A crucial factor during the negotiations will be the implications of several recently enacted laws, including the Balanced Budget Act of 1997, and the National Defense Authorization Acts of 1999 and 2000.

BBA-97 and NDAA-1999 provide for private sector compensation of federal agencies for costs of relocating federal radio frequency systems as a result of a reallocation of federal spectrum. In addition, a provision of NDAA-2000 specifies that the SECDEF, the chairman of the joint chiefs of staff, and the Secretary of Commerce must approve any spectrum reallocations and certify to congress that the reallocation will not result in any impact to national security.

Even if the 1755 - 1850 MHz frequency band is not allocated to IMT-2000, the Air Force isn't out of the woods. The international civil telecommunications industry has started planning for the Fourth Generation of telecommunications systems, which will require even more bandwidth.

AFFMA will be a central player in events surrounding the national decision on IMT-2000, and other issues regarding Air Force radio frequency spectrum access.

More information about AFFMA's mission is available at the agency's Web site:

http://www.affma.hq.af.mil/

Additional Third Generation, IMT-2000 and other spectrum information can be found at these Web sites:

NTIA: http://www.ntia.doc.gov

FCC: http://www.fcc.gov

## *Help Wanted*

**Pennsylvania ANG**

The 270th Engineering Installation Squadron, Bucks County, Pa., near Philadelphia has an opening in Ground Radio Communications (2E1X3) and Communications/Information Systems Engineer (33S3A). Active-duty service members who wish to separate from the Air Force, via the Palace Chase/Palace Front programs are also being sought. For more information, call Senior Master Sgt. M.J. Allen at DSN 991-1806, 215-443-1806, or send e-mail to marionjean.allen@pawill.ang.af.mil or Master Sgt. Donna Errickson, at DSN 991-1516, 1-800-997-2264 or send an e-mail to donna.errickson@pawill.ang.af.mil.

**California ANG**

The 261st Combat Communications Squadron, Van Nuys, Calif., has several part-time openings. They are: 2E1X1, 2E2X1, 2E6X3, 3C0X1, 3C2X1, 3E0X2, and 3E1X1. Cross training opportunities are available. You can use your Montgomery GI Bill with the Air National Guard Kicker Program to help pay for college. For more information call Master Sgt. Rich Maxted at 800-860-8456 or DSN 893-7300 ext 330 or send an e-mail to richard.maxted@cachan.ang.af.mil

**Maine ANG**

The South Portland, Maine ANG Station has part-time vacancies in the following career fields: 2E1X1, 2E1X3, 2E2X1, 2E6X2, 2E6X3, 2T3X4, 3C0X1, 3C1X1, 3E5X1. For more information, call Master Sgts. Tom Breault or Patrick Crowley at DSN 698-7904/03 or 800-549-9197. Tuition assistance is also available for Maine Air Guard members.

DEERE