July 2001

intercom

Journal of the Air Force
Communications and Information Community

Better ways of doing business

intercom

Volume 42, No. 7

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
Master Sgt. Ed Ferguson

Contributing Editor
Master Sgt. Seth McKeel

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.

better ways of doing business

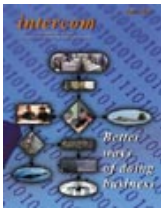
IA Awareness Campaign 2001

IT focus group

in other news

About the cover

This month's cover focuses on better ways of doing business



Cover by:
Jamie Ostrander & MSgt. Ed Ferguson

Are we there yet?

Understanding business processes enhances information flow

By Tech. Sgt. Terrence O'Brien
16th Air Force
Aviano AB, Italy

TSgt. Terrence O'Brien and MSgt. Lisa Haggett discuss training requirements for information managers.

Business processes, business rules, workflow, e-Works, iRIMS, TBMCS, IRIS, DMS, ASP, Coldfusion, MILMOD, XML, Dynamic HTML … "What language is that?" you might ask. These days even a simple discussion about anything work-related requires an understanding of the language SQL, server side scripts, and so on. The good news is learning a new foreign language has never been easier. The information management career field is evolving and we need to keep up with the changes.

The Air Force reminds us, "Flexibility is the key to air power." As information managers, we need to be flexible in our training, as the career field continues to progress with new technologies and tools. Our one constant is that we'll still handle information and the flow of it, whether we use the Web, Outlook or any other medium to get the job done. We'll accomplish the information life cycle mission with the aid of technology, and by establishing business rules and processes. We'll also need to look out for our fellow IMs and share what we know with them.

When I recently asked an NCO about her lack of training, she said she was too busy. My response to her, and you, is we don't have time NOT to train! We're all busy, and while tasks usually outweigh man-hours on any given day, training is too critical to be set aside or left incomplete.

After assessing training for the IMs in my own organization, I was alarmed by their lack of skills. We initiated an intensive program to bring their basic wartime skills up to speed, including computer-based training, discussion, hands-on demonstrations, examples and business processes. We emphasized information sharing as the most important part of IM. After completing this basic training, we got together with the local communications squadron to contract for advanced training.

Most IM operations are only one person deep, and we seldom have the luxury of two or three people in an office. Most of our supervisors are in another career field and don't know what's required of IMs. First we need to educate ourselves, and then our supervisors, on our career path. In my last assignment, I had to go outside the unit for training, guidance and mentorship. Every month I'd meet with my IM mentor to discuss ideas and problems. While I may not have always received an answer outright, I got a tremendous amount of guidance. We discussed things like business processes, the right way to approach business rules, and how to share information. One useful piece of advice, for example, was to have one copy of an item linked to a Web page, rather than keeping several on different hard drives around the office.

We talked about sending draft versions of EPRs and OPRs by e-mail, routing electronic staff summary sheets, creating templates in Outlook for common messages, putting the commander's calendar on the intranet and having it automatically updated by Outlook, using Outlook to manage suspenses, and creating templates for awards. In particular, we discussed using business processes and business rules to establish business practices. For example, when routing a document, we use tracking changes to record everyone's thoughts and comments.

We now use Outlook to monitor suspenses, by exporting the data to Excel and then graphing each section's on-time rates. By properly managing data, IM gives the boss a picture of how his branches are doing, where bottlenecks occur and the way manpower is being used, and branches are held accountable for suspenses. Each section can also see where it's spending its time.

As IMs it's our job to stay abreast of technology, and to become experts in the use of the tools of our trade (MS Office Suite, computer, network, and the Web).

See **BUSINESS PROCESSES** Page 4

Metrics helps put bombs on target

By 2nd Lt. Christopher Mendoza
83rd Communications Squadron
Langley AFB, Va.

Ever feel like you're stumbling around in the dark, not sure if you're moving forward or backward, or even moving at all? With information technology, it's often difficult to get a good sense of where we're heading. Our fellow airmen on the operations side of the house have an easier time gauging their progress. They can look out a window and quickly see that nine of 10 bombs landed on target, which is better than eight on the last mission. With information technology our targets are not bridges or bunkers, but rather delivering Global Command and Control System or e-mail services to deployed and in-garrison locations, or ensuring Information Assurance and availability of our information systems, among other services. How do we know if we're meeting our goals when the results are not as evident as a bridge that was or was not destroyed? Metrics are our window.

Metrics is a standard of measurement. In the comm and info world, it focuses on a particular characteristic of an information system's performance or efficiency. Metrics may be the amount of bandwidth used at a base during the duty day, or the amount of time a mission-critical system is available. What do these numbers really mean? What value do they have? How do they impact the warfighter? To serve as a window, metrics must be more than a simple measurement of performance or efficiency. Numbers have little meaning or value to anyone not versed in technical intricacies of a system. Metrics must clearly show not only system administrators, but also end users – the warfighters – how well information infrastructure and systems are operating. Useful metrics leads to better understanding of information systems capabilities, which leads to effective use of systems. Metrics identifies capability shortfalls, as well as superior performance. Identifying superior performance helps spread best practices throughout the system. At the same time, shortfalls can be corrected through allocation of appropriate resources.

The short version: Metrics provides focus and serves as our window on how we're doing. Next time another graph with metrics rolls across your desk, look at it as constructive feedback on how to either perform better or continue superior performance. If you create those graphs with metrics, keep in mind it must add value to what we do and be meaningful to the common user. Metrics shouldn't be created for its own sake.

Comm and info is the warfighter's enabler. While our primary mission is to provide communications and information services to warfighters, ultimately we're as responsible as pilots for ensuring bombs are on target. Ineffective use of our capabilities and poor understanding of our performance levels is unacceptable. Let's create and use clear windows to ensure we're putting bombs on target.

BUSINESS PROCESSES

From Page 3

Some action officers are better versed in PowerPoint than I am, and they've had the "just in time" training or the "I've got to know it now!" learning. These AOs constantly teach me tricks, but at the same time, I'm retraining them on proper ways of doing business, such as importing text or graphics instead of recreating them in the application.

If we learn to use the full potential of MS Office Suite, each program will let us import from, and export to, other programs. We must know which program is best suited to each facet of our job. For example, should we prepare a table in Word or a spreadsheet in Excel? Should we paste the table into PowerPoint, or link the spreadsheet to the PowerPoint presentation, so that updates to the Excel spreadsheet automatically update the PowerPoint presentation?

We've all done, or will do, briefings. What's the best way to link presentations in briefings? By creating a master slide with active links to each presentation, we can set or change the order of a briefing. When the briefer is ready to begin, click the link and the presentation will load. It then becomes the action officer's job to get the briefing to the correct location on the network or on a shared drive. Because you've made it a standard business practice, it's saved in the same directory with the same name every time. In addition, you're helping manage their data, and they're not managing your time. A briefer who arrives at the last minute is responsible for having the briefing saved in the correct directory under the correct name.

Never try to paste a PowerPoint presentation together. Inevitably, something needs to be changed. For instance, when you click on the master slide to fix the color on a particular slide and part of the presentation

See **BUSINESS PROCESSES** Page 5

How the DMS war was won: a true mission story

By Tech. Sgt. Jay Wilson
311th Communications Squadron
Brooks AFB, Texas

The Royal Guard, code named AUTODIN, had effectively dug into the trenches, and was there to stay. It had been in place for more than 62 years, with complete control over Defense Department personnel. Yes, the Automatic Digital Network was in power, and had to be taken out.

I'll never forget the day the commanding officer and his deputy, a couple of tough leaders by the name of Maj. Tim Hartje and Maj. Don Cosgrove, gave us the order. The mission was clear; AUTODIN had to be replaced at all cost. Complicating matters, we were told we wouldn't have our weapons. In fact, we'd have to face our fears head-on – it'd be a down and dirty, hand-to-hand combat mission. Still, Majors Hartje and Cosgrove gave us a boost. They assigned two combat-hardened information systems veterans by the names of Darryl Tolliver and Tim Condor to the group.

Casualty reports from DOD and all its entities didn't look good. We heard about similar campaigns to defeat AUTODIN that had resulted in the total wipe out of entire groups. DOD-established goals and projected dates of victory were being set back. The situation seemed hopeless.

Then it happened. The group known throughout DOD as "The Brooks DMS Strike Force" converted well over 95 percent of base units to DMS, beat DOD's target conversion date, provided hands-on DMS training for base users, and earned the base the Air Force's first DOD "DMS Pioneer" award. Reports substantiated the success of this crack group of comm commandos in waging the "Battle of Brooks," calming fears of the Brooks population by giving them the weapon of knowledge to overthrow the AUTODIN regime. Others throughout DOD starting calling upon our team for advice to launch successful attacks.

The day had come for Brooks when its people no longer had to succumb to the antiquity of AUTODIN by being forced to crawl, walk, drive or use one of those new-fangled scooters to visit a Base Communications Center. No longer were they be required to create high precedence messages, only to have AUTODIN's disk messaging process fail to deliver. Yes, victory was won! AUTODIN had been defeated, and in its place stood the Defense Message System.

DMS had freed the customer from AUTODIN's shackles by allowing customer convenience, ease of use, and guaranteed delivery of messages. It was easy to use as regular e-mail, and could be accessed right from the user's desktop computer. Unlike AUTODIN, DMS allowed the user to send attachments, have messages automatically re-routed to a specific location (in case the intended recipient was not available), and receive delivery notifications once the message had reached its destination. The possibilities were unlimited.

For their efforts, the DMS Strike Force – consisting of Senior Airmen Ryan Worthey and Linda McClintock, Airmen First Class Benjamin Otero, Jessica Hepworth, and Michael Wilms – received Air Force and DOD recognition. In fact, by the time you read this true war story, Airmen Worthey and McClintock will have visited Norfolk, Va., to accept DOD accolades for Brooks' successful campaign.

BUSINESS PROCESSES

From Page 4

turns pink in the middle or toward the end, this isn't a good thing. Everything may look great at the start of the briefing, until that pink slide shows up.

During one training session, I watched the instructor enter names from an access database into a Word document one-by-one to print letters for completed training. The training NCO said he didn't use Mail Merge because he didn't know how. It took me only a couple of minutes to show him what otherwise would have taken him a good hour to retype. The NCO had planned to take all this data back to Rhein Main to retype into a database. What's wrong with this? Why didn't he have an interactive database from the Web to pull the names down, Mail Merge the data, and automatically update the records? Again, he didn't know what I was talking about and he hadn't heard of Data Access Pages or Active Server Pages.

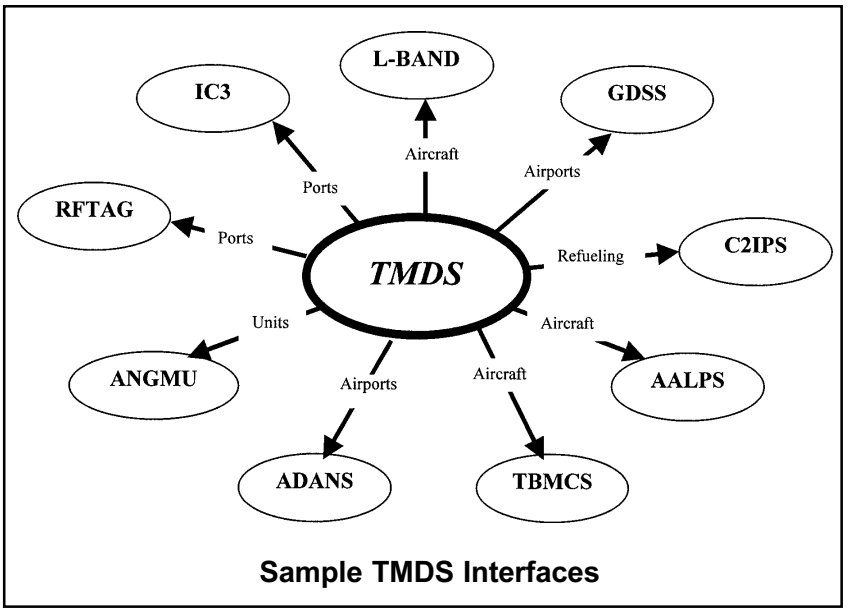
Data Access Pages and Active Server Pages take a little more work, but the payoff is enormous in time saved. Anywhere the trainer goes, he can access and update the data, and print the training letters from his database. All he needs is access to a "dot mil" site. This is a huge workload reduction – the same work results in about half the time! Granted, one must learn the applications, but isn't that our job? These are the tools of our trade, and shouldn't we know them well? You don't expect to have a pilot fly a plane without training. Pilots are constantly training because staying proficient is their job. They're always being evaluated on different tasks and tactics. That's how we should train.

See **BUSINESS PROCESSES** Page 7

Table Management Distribution System makes data synchronization easy

By Capt. Dan Liggins
Architectures and Integration Division
Directorate of Communications and Information
Air Mobility Command
Scott AFB, Ill.

In 1994, Air Mobility Command's Communications Directorate staff at Scott realized they had a problem. Their high technology, state-of-the-art command and control systems were talking, but didn't understand each other. To get a handle on the problem, AMC communicators decided to analyze message transactions for a year between three key systems: Command and Control Information Processing System, Global Decision Support System and AMC Deployment Analysis System. The situation was worse than they originally thought…they estimated as many as 50 percent of their messages were being rejected. Even more startling, the systems were working exactly as designed. So what was the problem?



Sample TMDS Interfaces

The problem was AMC's C2 systems were developed and fielded with different reference data tables and data element relationships. Reference data are simply standard domain values that are common across multiple automated information systems. For example, "C-130" would be a reference for a C-130 aircraft. The C2IPS, GDSS and ADANS used dozens of reference tables to validate data that flow across the system interfaces. We found that the reference data didn't match (i.e., a C-130 was represented by "C-130" in one system and "C130" in another), and then messages containing these data were rejected. What caused this? The importance of standardized, synchronized data was not initially recognized during the system development process. The result – approximately one out of every two messages was rejected, and didn't reach AMC and warfighting CINC decision-makers.

AMC aggressively pursued an enterprise-wide approach to solving the problem, and in 1995 the Table Management Distribution System was born. TMDS is a Web-based information system that synchronizes reference data among operational systems. It distributes the tables to operational systems through replication, flat files or direct pull. Its purpose is to provide centralized control, maintenance and distribution of reference tables to operational systems. The effort decreased message rejects from 50 to 7 percent. Combined with other enterprise efforts – the Command and Control Interface Design Document, which standardizes business rules at the interface level, and the Logical Data Model, which standardizes data elements at the database level – it decreased data related rejects to an astounding .02 percent! Additionally, where it previously required system administrators two weeks to update reference tables, with TMDS it takes less than an hour.

The secret to TMDS' success is the crack team of data analysts, application developers and database administrators that keep the process running like a well-oiled machine. This customer-oriented 16-person team is on call 24/7, and works closely with functional managers and system administrators to ensure data are sent and received in a timely manner. They work with functional managers every day to update and maintain domain values for over 600 reference tables. They also work directly with system administrators to develop system-specific table structures and translations for the tables. Simply, system administrators tell the TMDS staff what data they want, what format they want it in, how they want to receive it and how often. The TMDS staff does the rest, and relieves administrators from having to translate data at the receiving end. Now that's customer service!

AMC's TMDS effort experienced such phenomenal success that U.S. Transportation Command got into the act. In 1999, TMDS began synchronizing USTRANSCOM systems and currently manages 180 of their reference items. In 2001, AMC hit another milestone with its data synchronization benchmark: It be-

See **DATA SYNCHRONIZATION** Page 7

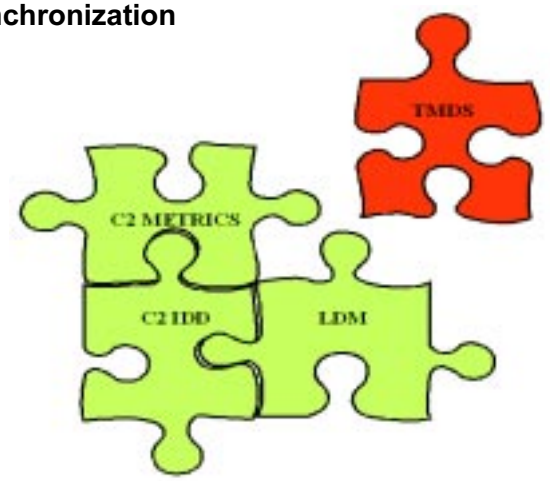
DATA SYNCHRONIZATION

From Page 6

gan the Joint Reference Table Logistics Pilot project, a 12-month test in which the TMDS team manages approximately 450 reference items for the Defense Logistics Agency and will interface with up to 10 systems. The plan is to use this pilot as a model for DOD-wide implementation upon completion, a move that's currently being considered by the Defense Information Systems Agency.

Among systems it interfaces with, TMDS has all but eliminated interoperability problems due to data synchronization. Its performance results speak volumes and, as awareness of the system grows, it should have little problem gaining converts throughout DOD.

AMC's Enterprise Solution to Data Synchronization



BUSINESS PROCESSES

From Page 5

We first get the basics from tech school and on-the-job training, and then we need a mentor to guide us along the way. However, mentors probably aren't going to come looking for us – we'll have to go looking for them. The mentor should be an NCO who's willing to spend time with us for hands-on training, career guidance, keeping a positive attitude, and possessing some well-grounded skills, while keeping an eye on the future. It isn't always what jobs you can get or the positions that you hold, it's what you bring to the fight, always remembering it's during peacetime that we must practice for war.

My boss keeps me focused on how any process I develop will help him win an air war. If it hasn't any added value, it really isn't worth the time. I've learned a lot from this. I can do some pretty cool stuff, but it always comes back to the basics: black type on a white background, information on a page. But no matter how pretty it is – or isn't – it's the information itself that counts. Is it timely, in the right format and directed to the right person to make a difference?

The Web is a great way to share information, and we constantly hang information out there for others to use. The problem is that we suffer from information overload – everything from how to sell something, to how to make a million bucks, trade stocks or search for our ancestors. It's our job to sift through the plethora of information, find what's important and present it in the form of coherent, relevant thought, assuring that it's not just more useless information. Everything we put on the Web must serve a need and be current. Having to constantly update our information can be a daunting task. We should lean toward using databases and links to our working documents. Why not have links to our directory to search for the most current document through the Web?

You can turn on Web browsing, place documents in the appropriate directories with an electronic file system (iRIMS is coming), and there you have it. You need some sort of electronic filing system for your documents. We have an e-records directory, and every section has a folder, and each section files items in their own directory. However, they can also search other directories if necessary. We've even put this file system to use on Outlook and the Web. We created folders with tables and rules according to our approved file plan, then on the Outlook Tool Bar we added these folders and started dragging and dropping whatever needed to be filed.

If your boss is used to seeing his favorite "stuff that was done" folder, just rename the shortcut on his Outlook tool bar. What he calls it won't matter, because he'll be dragging it to the right place where you can manage the information. You'll see redundant information in these folders which you can delete – the same e-mail can be filed over and over again, though all you see is copy (2) copy (3) and so on. That's the point when you start managing data. You only need one copy of a document, everyone reads off the same document, and no one gets misinformed or blindsided. Now this doesn't happen overnight, because it takes time to train users. But even if it's front-loaded, this will save time in the long run if you keep the information in a central location where it's easily managed and secure. You can search by author, title, subject or text item. Granted, you might get quite a few hits on your search, but you'll find the information if it's properly filed, and not in someone's personal PST file.

As our career field continues to evolve, training is crucial to our success. We trained as 702s, and we need to keep training as 3As. Our primary job is still information, but now we can use technology to leverage information management. It's important to keep our wartime skills sharp, for ultimately that's why we're training, and we need to train like we fight. Having the basic skill sets makes it much easier to get up to speed during a conflict when we're required to augment other units. Remember that each of us – not someone else – is in charge of our own career. The training is available – we just need to go get it.

USAFE AIRPS leverages technology to improve service

By Roger Kolkena
Air Postal Squadron
U.S. Air Forces in Europe
Ramstein AB, Germany

The U.S. Air Forces in Europe Air Postal Squadron is aggressively applying technology to advance the way it moves mail, manages resources and serves customers. Several initiatives designed to reduce workload in USAFE post offices are being evaluated and most will be implemented by the end of this year. The AIRPS is working the efforts in close conjunction with the Military Postal Service Agency and the United States Postal Service.

USAFE post offices are testing options to automate package tracking and delivery management. Until now, delivering packages required postal clerks to use an error-prone four-step procedure: place parcels on a shelf and annotate location, write out delivery notices, sort notices, then place notices in recipients' post office boxes. Under the new process, parcels will be scanned with optical character readers. Delivery notices will be computer generated in post office box sequence for clerks to place in customer boxes.

USPS is examining better sorting methods to send mail to each Air Force Post Office in post office box sequence, allowing post office personnel to place mail directly into customers' boxes without sorting. By eliminating the need to repeatedly sort mail from the five-digit Zip code down to box sequence, APO mail clerks will touch each piece of mail just once.

The Automated Postal Locator System will be a Web-based database maintained by USAFE AIRPS that will replace 42 separate locator databases currently on stand-alone computers throughout the command. APLS will enable mail forwarding between APOs, saving money and time. By taking the system one step further, APLS data may also be used to identify address changes before mail enters the mailstream, reducing mis-addressed and undeliverable mail to Europe by 30 percent.

Photo by A1C James L. Harper Jr.

SrA. Kevin Dunn, postal worker, 48th Communications Squadron, stacks outgoing mail.

Photo by Staff Sgt. Lori M. Stewart

Staff Sgt. Derrick Cauthen, postal advisor, 363rd Expeditionary Communications Squadron, processes packages to be mailed.

The Automated Military Postal System is a Web-based repository for key postal data such as financial, logistics, personnel, service hours and inventory. The system was developed by MPSA, will interface with USPS data systems, and will produce most required monthly and quarterly reports. AMPS will save postmasters many hours of data gathering and report writing.

Postal specialists use a different approach to training than is used by other commu-

USAFE AIRPS

From Page 8

nications specialties. The 8M000 special duty identifier has no skill levels to designate degree of expertise, and no career development course. USAFE AIRPS has prepared a 13-volume series of training pamphlets and tests to teach and evaluate trainees, but successful results demand substantial supervisor involvement, and trainee development can be hard to validate. To produce better, more consistent outcomes, the command is moving pamphlet material to a Web-based training system. Computer based training will require trainees to master each objective before proceeding, and will give them instantaneous performance feedback. By centrally tracking completion, postmasters and command postal officials will have progression data to ensure trainees advance in a timely manner.

A method for collecting useful, reliable customer comments is essential to process improvement. To help generate meaningful trend data, USAFE intends to implement the Interactive Customer Evaluation program, an Army innovation adopted by DOD. Instead of hand-writing feedback cards, customers will respond through ICE on line or at dedicated terminals in post office lobbies. ICE provides postal managers at all levels with real-time customer satisfaction reports, cumulative data for organizational planning, and analysis of customer data for trends.

These initiatives will reduce repetitive tasks for post office personnel and help make the post office more responsive to customers' needs. With them, postal leaders will have the power of technology to ensure mission accomplishment.

Flight provides comm & info support to Spangdahlem

By Senior Master Sgt. Stephen Burn
52nd Communications Squadron
Spangdahlem AB, Germany

Many people at Spangdahlem – and especially those assigned to the base's geographically separated units – may have reason to believe they're at the lowest priority level to receive new communications and information services. A common frustration is the long lead time required to upgrade comm and info systems. Providing comm and info support to the GSUs holds many challenges. A recent planning and implementation workshop at Air Force Communications Agency, Scott AFB, Ill., presented an opportunity to share how USAFE supports comm and info needs of these remote locations.

In May, Master Sgt. Raymundo Custodio, Directorate of Communications and Information, HQ U.S. Air Forces in Europe, Ramstein AB, Germany, and I represented USAFE in the P&I process-oriented description workshop. Its primary objective was to update the Air Force Manpower Standard for the P&I work center, which was last done in 1994. Many of the processes outlined in the P&I manpower standard were easy to validate because they're performed at every main operating base.

Spangdahlem's successful use of technology was key to overcoming logistical challenges to rapidly deliver comm and info services to the GSUs, in addition to supporting their main operating bases. As a result, Spangdahlem's experiences provided some valuable lessons learned for the workshop forum.

Many base-level processes involve P&I oversight – the foundation of project management. However, the P&I function does much more. Essentially, planners manage transition strategy from baseline architecture to target configuration. In other words, the P&I flight charts modernization strategy for the comm and info systems environment. Out with the old, and in with the new!

USAFE's mission as a forward-deployed command required it to develop positive additive variances to quantify additional workload. The primary workload variance for Spangdahlem was GSU support for over 80 different sites – a significant source of workload. For example, the 52nd CS P&I flight aggressively planned and implemented communications infrastructure upgrades for all its GSUs. These efforts include installing fiber optic footprints at munitions support squadrons and virtual private networks, allowing distant subscribers to ride the NIPRNET backbone to achieve SIPRNET capabilities.

Spangdahlem is taking bold steps to compress the timelines to implement these projects and project wing comm and info capabilities to their GSUs. Extensive efforts are under way to automate the comm and info requirements process for Spangdahlem, which will accelerate implementation of new GSU capabilities. Both AFCA and AFMIA were impressed with the support to the GSUs.

The recent P&I process-oriented description development workshop confirmed and validated contributions the P&I flight brings to the fight. Each command sent experts to draft a framework for the new draft manpower standard for the P&I flight. The forum also identified potential improvements, initiatives and workload variances. After four contentious days of collaboration, we completed a new draft manpower standard for the base level P&I function.

Though significant progress was made, the reengineering study for this function needs more analyses, measurements, multiple MAJCOM/FOA/DRU reviews, and approval of AF/SC and the corporate structure. Chief Master Sgt. James Harris, chief of AFCA's unit support branch, and a workshop participant, said, "I think we'll see a very positive result from developing the new P&I process-oriented description."

Document imaging system helps unit go paperless

By Cheryl Stefenel
552nd Computer Systems Group
Tinker AFB, Okla.

A new document imaging system is coming on line to help the 552nd Computer Systems Group go paperless.

The group's DIS initiative is in keeping with the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996. The system is compatible with the technical order digitization effort, and will bring the group into compliance with Department of Defense objectives under DOD's Logistics Strategic Plan mandate to be fully digitized by 2002.

DIS will be accessible to the entire 552nd Air Control Wing by September. It will maintain technical library documents, such as contracted and internally produced user manuals, design documents, and technical design documents. Information will be received from Air Force organizations, Airborne Warning and Control Systems contractors, Oklahoma City Air Logistics Center, NATO organizations and other DOD agencies, and stored in a database, said Johnita Guidry, documentation office, 552nd Computer Systems Squadron's Configuration Management Section.

Guidry said developers, configuration managers, program managers and external organizations have a need to collaborate on DIS information. "System users will have a rapid access information search tool and data library. It'll be an engineering repository of information, both current and historical, for research and development supporting the $9.6 billion AWACS fleet," Guidry said.

DIS will also free up scarce resources for other mission activities. Using LaserFiche software, records will be retained on line in full text and image format, and will be available to all users by e-mail, network browser or application interfaces. Documents will be reproduced or printed only as required.

Documents are currently accessible on the local area network, and will be available later on 4 mm tapes, and writable and rewritable CD-ROMs. Data will be portable to any supported media standard. Guidry noted DVDs will be supported when hardware is feasible. Products on CD-ROM media will be distributed to rapidly access and research documents as required.

DIS will reap many benefits, Guidry said, including making more storage space available, reducing duplication of effort, and cutting costs for paper copies. In addition, document control, revision and distribution will be more efficient.

Portal key to providing agile combat support

By Capt. Samuel D. Bass
Commander, Software Engineering Flight
AMC Communications Group
Scott AFB, Ill.

By now you've heard about the Air Force Portal and its potential for revolutionizing the way we conduct business in the Air Force. Since becoming involved in the Air Force Portal in December, I've tried to stay on top of developments to keep my programming flight ahead of the proverbial power curve. What I've come to realize, however, is that there are many perceptions of what a "portal" is, and just as many ideas about what the Air Force Portal should become.

This article explores some portal basics and encourages people to support this incredible opportunity. It begins with a definition of a Web portal, describes a few commercial portals, highlights some themes common to corporate portals, and concludes with content management.

A Web portal is a user-specific and dynamic Web page, viewable with a Web browser. The most effective portals can be viewed with any Web-capable device, including digital phones and hand-held computers.

I have several commercial portal accounts, including Yahoo, CNN, AOL and Excite. Since the concept of a portal is to get all the information you want by viewing a single page, I rely on a single portal. On any of my portal accounts, I can select and arrange small information applications or modules tailored to my interests or geographic location. These modules are building blocks that create a complete page of customized information.

For example, when I log on to my portal, I see the weather forecast for Scott and a few other locations around the world, this week's local theater listings, tonight's television schedule for my cable provider, my e-mail inbox, current value of stocks in my portfolio, my tirelessly collected and organized Web page bookmark collection, and news articles on my favorite topics. No matter where I am when I log on, all I need to access this information is a computer with a Web connection.

The content is tailored to my own preferences and, with the exception of some advertising and mandatory content, I control the layout and appearance of my portal page. This is a great recreational portal that has replaced my daily newspaper, but how do businesses use the portal model?

According to various sources of information on corporate portals, or *corportals* as they're sometimes called, several traits are consistent to a successful Web portal. I list seven more common ones in the accompanying side bar.

Yahoo's Web Directory is an example of the traits *searchable* and *categorized*, and its portal has the traits

personalized and *secure*. Corporate portals have content of use to specific job areas within the organization, like marketing or production, but also provide content useful to people across the organization, like travel expense reporting and leave management. Corporate portals leverage *integrated applications* by using Web-based forms to complete transactions, avoiding reliance on client-based form filler applications and cumbersome form template libraries.

Getting rid of legacy applications and streamlining information distribution channels are two inexpensive ways to improve profit margins in the private sector. In the Air Force, these efficiencies translate to mission effectiveness and enhanced information management.

The promise of the Air Force Portal extends far beyond Web-based form completion, however. Being able to access systems around the Air Force from a common point that handles accompanying security issues will lighten the load for users who otherwise have to deal with dozens of user accounts and passwords. Additionally, the modular portal architecture will result in a common interface to all of these systems, easing training requirements.

As communications and information professionals, we must understand what makes portals effective in commercial and corporate environments in order to ensure the Air Force Portal is successful and useful across the Air Force.

As the Air Force Portal matures over the next few months, comm and info professionals will play a critical role in helping users leverage content to make their jobs easier. Project managers Air Force-wide are responsible for identifying systems for eventual migration to the Air Force Portal. Without a clear understanding of what it means to be "on the Air Force Portal," successes in that migration will be random.

To mitigate that risk, we in the Software Engineering Flight have become what I call Portal Evangelists. We learn all we can about Web portals and their capabilities, and keep up to date with the Air Force Portal by attending developer's conferences and reading online documentation. As we meet with customers from around Air Mobility Command, we ask them about their plans for the Air Force Portal. If they respond with a confused look, we explain the benefits of the portal model and, if appropriate, convince them that building a Web-based solution is the only way to go.

As our customers learn about Web-enabled applications and how they might fit on the Air Force Portal, they bring us great ideas that might benefit people Air Force-wide. It's our job to turn those ideas into portal content that won't obscure portal effectiveness. Unfortunately, too much content can become a problem.

Because the term "portal" means different things to different people, each major command appointed a content manager. This person is responsible for identifying systems that could be migrated to the Air Force Portal, coordinating and staffing migration, and providing funds for the development effort.

The content manager needs to truly understand the portal model, and will weigh the user scope of individual portal components against cost of development.

One of the more important issues for the content manager is the *categorized* architecture of the portal, which is second on the list of Seven Traits of a Portal. To help users find information they need to do their jobs, the content manager ensures portal modules are organized in a logical manner. For the Air Force Portal, this organization might be along functional, geographical or MAJCOM lines.

The Air Force Portal should have mandatory content for each user's portal page. Mandatory content should be limited to information of importance to every member of the Air Force or MAJCOM, so effectively managing this content will be essential to prevent the "Commander's Corner" module from being ignored like so many banner advertisements. The ultimate purpose of mandatory content is to disseminate information, which is a core reason for establishing a portal in the first place.

As Air Force Portal content grows, content management issues will become critically important. Content managers and content developers must work together to ensure Air Force Portal content is consistent with goals of the major command.

Understanding the portal model and top-level issues like content management will ensure Air Force Portal deployment is successful. We've taken the first few steps on a long journey to realizing the promise of the Air Force Portal.

Oracle CEO Larry Ellison said "the network is the computer," but I say the portal is the computer. With smart content management, the portal will enable our warfighters to use thin clients or even hand-held computers, lightening our deployable load. For communications and information professionals, providing agile combat support is job one. Why not let the portal carry the load for us?

Seven Traits of a Portal

-**Searchable:** the user can find the information needed to do the job.

-**Categorized:** information is organized logically to enhance dissemination.

-**Collaborative:** facilitates information and idea sharing with on-line work centers.

-**Personalized:** information is tailored to a person's role, habits or preferences.

-**Role-based:** available content is dependent on the role of the user.

-**Integrated Applications:** information can be shared via Web-based forms and tools, without relying on specific applications.

-**Secure:** access to information necessary for the user to do the job is strongly controlled.

Wireless wilderness alters spectrum processes

By Joe Sulick
Air Force Frequency Management Agency
Washington

They're everywhere – billions of 'em. Everyone wants something wireless, because cables "aren't cool;" something real-time, because things happen fast; and something useful and accessible anywhere.

Rapid advancements in wireless technologies – especially in macro-trend areas of integrated circuitry, signal processing capabilities, and digital systems – are demanding global spectrum access. This global economic wireless explosion impacts military operations because there's little free spectrum available for new services; and that constrains military testing, training and operational mobility. Compounding the problem, current spectrum legislation dates from 1934! A different world then: no Playstations, or Nintendos, or Blackberries. No TV! Yikes! How can we adapt 1934 spectrum processes to the 21st century wireless explosion?

Congressional legislation over the past decade reallocated a lot of federal spectrum for auctions to the private sector. This contributed to the wireless explosion – a world predominantly populated with systems that employ all digital, software-controlled technologies. Systems will be self-managing, adaptive and dynamic in the sense that their operational behavior related to spectrum management – such as frequency, power and bandwidth – can vary dramatically and rapidly over time. This evolving paradigm, based on sharing and adaptive technologies, will overrun current dedicated user technologies and serve the Department of Defense faster, cheaper and better.

One highly visible emerging DOD communications technology, the Joint Tactical Radio System – and other less visible, militarily significant emerging technologies, such as ultra-wide band systems and space systems developments – set the stage for the next generation of "right stuff" for military operations. These also offer challenges and opportunities to which the spectrum community must adapt.

JTRS and other software-defined radios illustrate the DOD commitment to developing advanced communications systems to more efficiently access this scarce military operations resource. It represents the new breed of radio: modular, scalable, software re-programmable, affordable, high capacity, and providing both line-of-sight and beyond line-of-sight information capabilities. It's a major step forward in capacity to support information transfer requirements of the modern battlefield. This concept will achieve performance by employing re-programmable software, and frequency-agile and demand-adaptive technologies, to handle a variety of data transfer demands. It represents opportunity. It embodies many advanced technology concepts to form a basis for future spectrum management policy: interoperability with commercial services, software control, configuration adaptability, and ability to operate over a wide frequency range. The software that will be the brains of software-defined radios will control the way the radio performs, as well as its behavior in its intended operating environment. Some technical characteristics likely to be implemented in the software are modulation type, transmitter power and bandwidth, network access control and keys, national and international spectrum allocations, host nation approval to operate, and most of the experience and ability of an on-site spectrum manager. The challenge is to incorporate this knowledge base into the radio and ensure that it's supportable and can be spectrally certified without any critical restrictions.

Ultra-wide band technology also has potential for a breakthrough in wireless systems. This technology sends information on tiny wave pulses rather than continuous radio waves. This implies smaller devices that do more. It employs tens of millions of energy pulses spread across the spectrum. The technology has potential to produce significant benefits to DOD, including increased communications capacity; smaller, cheaper and less power hungry components; lower probability of intercept; and increased accuracy. Similarly, space-borne applications represent a potential growth opportunity that can be exploited by DOD for the use of spot beam antennas. Highly-directive, phased-array antennas aboard the satellite will maximize frequency reuse.

New stuff like software-defined radios, UWB, and others provide the spectrum management community an opportunity to reengineer current certification business processes to encourage and exploit emerging technologies. Sharing, reuse and real-time, are terms that will alter the spectrum environment and contribute to our ability to meet increased global demands for our military operations.

They represent major breakthroughs in electronic technology and embody the coming bandwidth revolution – the paradigm shift to a speed-of-light world. DOD spectrum managers must evolve as system application and interoperability managers, and become proactive to upgrade emission level standards and create more dynamic spectrum allocation tables – for global operations. The spectrum community must prepare to conduct warfare in a shared spectrum environment, and develop new processes to adapt to a constantly changing environment.

Sound COMSEC practices provide edge over enemies

IA: life or death on the battlefield

By Col. Michael E. DeHart
Director of Communications and Information
Air Force Special Operations Command
Hurlburt Field, Fla.

The term Information Assurance has supplanted communications security as the phrase of choice for protecting information, but COMSEC is still at the heart of every Air Force operation, mission or contingency, protecting information and ensuring successful employment of our forces. Nowadays, COMSEC is a major component of IA that affords us an asymmetrical advantage over our adversaries. Whether deployed or in-garrison, implementing sound COMSEC practices is integral to global Information Assurance and Information Superiority.

Recent and earlier high-profile security incidents affecting our national security interests serve as painful reminders of how acts of espionage by our team members have cost others their lives. This is but one of several weak points involving the protection of our secrets. More often than not, whether intentional or unintentional, people make or break the effectiveness of our established COMSEC programs. I urge every Air Force warrior to do your part in safeguarding your computer networks and communications assets from exploitation and compromise. Take the time to question the unknown, especially when you suspect that a potential problem lies ahead. Commanders, supervisors and comrades all depend on you to do your part in exercising sound COMSEC practices.

Our networks must be accredited to the classification level of information placed on them. One of the most troublesome trends affecting our networks today is the inadvertent transfer of classified information onto an unclassified network. This issue is one we must face head-on by thoroughly examining the source of all information prior to introducing it into our networks. Your base Information Assurance and COMSEC offices can provide you with valuable educational tools and guidance to prevent COMSEC incidents.

Our ability to protect our communications assets and processes could be the difference between life and death in the air and on the battlefield, so as we charge into the future with new and emerging information technologies, it's crucial that we integrate Information Assurance into our planning.

Plan helps ensure proper destruction of COMSEC materials during emergency

By Harry Wildermuth
Computer Systems Office
Air Force Materiel Command
Wright-Patterson AFB, Ohio

You're not sure what's happened, but suddenly the plane you're flying in goes into a steep nosedive, headed straight towards the sea. Luckily, the pilot and co-pilot are able to regain control and safely land on the nearest island. Not so luckily, the nearest island happens to be foreign territory. Meanwhile, the crew frantically gathers communications security keying materials and destroys them as quickly as possible to prevent unauthorized access by authorities who immediately take custody of the aircraft. While this may at first seem to be an unlikely scenario, it's not unlike recent experiences of one U.S. Navy aircrew.

We know how important it is to secure our information systems. It's equally important to prevent access by destroying COMSEC materials on time, and by having established procedures for emergency situations. It's paramount to protect our resources from capture by our adversaries.

To protect our cryptographic resources in emergencies, each user agency is required to have an emergency action plan, according to AFI 33-211, *Communications Security (COMSEC) User Requirements*. EAPs are designed to guide users in taking required action in case of an emergency, such as fire, natural disaster, bomb threat or hostile actions. For fire, natural disaster and bomb threats, EAPs normally consist of securing the COMSEC materials and evacuating the area. Overseas locations and deployed units are also required to plan for hostile action, including procedures for precautionary and emergency destruction of COMSEC materials.

If you're at a base or forward operating area and hostilities occur, under the EAP, the commander could direct facilities holding COMSEC materials to implement precautionary destruction. It includes materials not required for continuous operations, but not equipment. The next question is, what material do you destroy first and why? The answer is superseded COMSEC material. The reason is, if an enemy captures your facility they would be able to, with the right equipment, retrieve all information that was transmitted and received over the COMSEC equipment during the time frame the superseded COMSEC material was used. This could be anywhere from just a few to several thousand classified mes-

See **COMSEC DESTRUCTION** Page 15

COMSEC

Reporting deviations vital to national security

By Harry Wildermuth
Computer Systems Office
Air Force Materiel Command
Wright-Patterson AFB, Ohio

For anyone who uses communications security materials, it's vital to know how to identify and report COMSEC deviations. When COMSEC materials aren't handled, stored, controlled or destroyed properly, you have a COMSEC deviation. Knowing COMSEC policies and procedures makes it easier to identify deviations.

It's important to report COMSEC deviations so officials can determine the potential harm to crypto systems and national security. Reporting procedures follow AFI 33-212, *Reporting COMSEC Deviations*.

What would you do if you found an unattended safe left open that contained COMSEC materials? First, you would immediately perform an inventory to see if anything is missing. You would then secure the material in another COMSEC safe and notify the COMSEC Responsible Officer or alternate. The CRO notifies the COMSEC manager and unit commander. The COMSEC manager and CRO gather all known information and determine what type of deviation has occurred. The COMSEC manager then advises the controlling authority of the keying materials and COMSEC equipment involved.

The controlling authority determines whether the keymat has been compromised. If there was no one else in the area and the keymat showed no signs of tampering, the controlling authority would probably determine there was no compromise. However, if the keymat was missing then all keymat holders would be notified and the keymat superseded.

Meanwhile, the commander of the violating unit appoints an inquiry official to interview all personnel and organizations involved and gather information. The inquiry official's report to the commander provides findings and recommendations. The unit commander provides comments and either concurrence or nonconcurrence with the recommendations.

The COMSEC manager then reviews the report, provides additional comments, and concurs or nonconcurs. The COMSEC manager converts the final report into a message, including an Air Force case number. Once the final report is sent, the controlling authority provides an evaluation of the incident. The MAJCOM reviews the final report and the controlling authority's evaluation, and reviews the reports to ensure sufficient corrective action has been taken to prevent reoccurrence, then recommends case closure. HQ AFCA reviews the final report, and all correspondence relating to the case, and once all actions are completed, closes the case.

There are many types of COMSEC deviations, and anyone who deals with COMSEC materials must be trained to identify them. It's important to remember to report deviations to the CRO or COMSEC manager, rather than the information security manager. Carelessness and insufficient training cause most COMSEC deviations. The bottom line is they don't send you to jail for causing a COMSEC deviation, but they might if you try to hide it.

COMSEC Terms

COMSEC Deviation – An occurrence involving failure to follow established COMSEC instructions, procedures or standards.

COMSEC Manager – Person responsible for managing COMSEC materials assigned to a COMSEC account.

COMSEC Materials – Items designated to secure or authenticate telecommunications. COMSEC materials include, but are not limited to, keys, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic, and other items that perform COMSEC functions.

COMSEC Responsible Officer (CRO) – Individual within an office or area responsible for COMSEC materials received from the COMSEC manager.

Controlling Authority – Official responsible for directing operation of a cryptonet, and for managing operational use and control of keying materials assigned to the cryptonet.

Keying Material (keymat) – Key, code or authentication information, in physical or magnetic form.

Tips outline proper use of secure telephones

By Terry Sweat
16th Special Operations Wing COMSEC Manager
Air Force Special Operations Command
Hurlburt Field, Fla.

Because of inherent missions of special operators at Hurlburt Field and sensitive operational information generated by these missions, many of us need to use secure communications to transmit voice and data information. For anyone unfamiliar with secure telephones, here's a brief background on the phones and their use.

The Secure Telephone Unit and Secure Telephone Equipment provide secure voice capability for discussing and transmitting classified, or sensitive but unclassified, information. The main differences are data transfer speed and sound quality. STUs operate in analog mode; STEs operate in digital mode. STUs use a crypto-ignition key; STEs use an encryption card. The STE has a clearer connection. Both are Controlled Cryptographic Items and unclassified when the CIK or encryption card is removed.

Classified information should not be transmitted on a STU or STE when:

- There's a question of validity of authentication information in the display window.
- There's doubt of validity of the organization where the distant phone is located.
- The display indicates the distant phone's CIK or encryption card has been expired for more than a reasonable period of time (e.g., two months).
- The display indicates the distant phone contains a compromised key. (This is a COMSEC reportable incident.)
- The display fails.

Remember to follow these security tips when using your STU or STE:

1. All personnel assigned to an area where classified work is accomplished must have an appropriate security clearance. When this isn't possible, implement procedures to prevent uncleared persons from hearing classified face-to-face or telephonic conversations.

2. Don't exceed the classification level on the phone's display.

3. Remember to remove the CIK/encryption card from the phone after each use unless the phone is located in an appropriately classified open storage area.

4. When the CIK/encryption card isn't in use, secure it in a General Services Administration approved container. If not available, the CIK/encryption card must be in personal possession or stored in a locked drawer – in a separate room from the phone.

5. When using phones in data mode, remove classified information on the screen as soon as possible.

6. All STUs/STEs located in private residences must have a residence CIK/encryption card. Display window must read residence when phone is keyed. All residence CIKs/encryption cards must be in personal possession when not in use.

7. Protect a keyed STU/STE at the appropriate classification level. An unattended STU/STE with the CIK/encryption card inserted must be in an area approved for open storage at the classification level of the key. STUs/STEs left unattended and not in an approved open storage area must be reported as a deviation.

For further guidance, contact your unit STU/STE Responsible Officer or base Communications Security Manager.

COMSEC DESTRUCTION

From Page 13

sages that might be compromised if the enemy gains access to the superseded material. So you see why it's important to destroy superseded keying material. You would then work on destroying current, and finally future keying materials.

Emergency destruction goes hand-in-hand with precautionary destruction. An ideal situation is to be notified of a possible attack and implement precautionary destruction first, reducing your COMSEC material holdings. So when the hammer drops and the perimeters are falling to enemy attack, emergency destruction of the remaining materials will be a lot easier than having to destroy it all at once. Emergency destruction on board an aircraft is one of the fastest to perform. Normally, aircraft flying near or over hostile territories are flying with minimal COMSEC holdings, so precautionary destruction is usually not required. However, aircrew members must be thoroughly trained on, and ready to perform, emergency destruction procedures.

Users must understand that emergencies can result in loss or compromise of COMSEC materials. Planning can prevent or reduce risk potential and help users cope with emergencies. When preparing your EAPs: keep them realistic and simple, and include measures to assure materials remain secure until they're destroyed. An important part of your plan is to include periodic dry run exercises to assure everyone involved is able to perform all the tasks. Performing required actions should become an automatic response. A good emergency destruction plan could prove to be the vital link in protecting our secrets from our foes. Do you know what to do if an emergency arises?

Lost identity becomes airman's worst nightmare

By Master Sgt. Jim Greeley
Airman Magazine

Identity thieves cash in many different ways, but the end result is the same — red tape, pain and heartache for victims.

His wedding ring and his combat boots. That's what the crook left in Senior Airman Will Armstrong's gym locker. Everything else was gone — car keys, house key, uniform, squadron hat and wallet. Gone.

The date is burned into his memory — Nov. 17, 1999 — the day he lost his identity.

"It's been a living hell," said Airman Armstrong (not his real name).

When he was first ripped-off Airman Armstrong was angry more than anything else. How could someone cut the lock off his locker, in a high traffic gym, on a secure Air Force base? Fortunately, everything could be replaced. At least the thief was "nice enough" to leave his wedding ring.

Airman Armstrong took, in his mind, the right steps. He canceled his credit cards, called the bank and filed a police report. Inconvenient and a hassle, but not that bad, said the newly married airman.

In truth, his nightmare was just beginning. The phone calls started two months later.

"Car and boat dealers were calling," Airman Armstrong said. "Collection agencies were threatening me, and banks were calling to say I was bouncing checks all over town. I was scared."

He called the local cops for help and discovered there was a warrant out for his arrest. Fear turned to terror. Airman Armstrong turned to the Air Force Office of Special Investigations.

"We discovered this thief was living large off other people's money for a decade," said Clint Cantrell, OSI special agent who collared the guy who stole Airman Armstrong's wallet and identity. "This guy was part of an identity theft ring in New York and New Jersey."

More than 500,000 people will fall victim to identity theft this year, according to government estimates. Currently, the Air Force doesn't track statistics on identity theft victims, but OSI officials said the number of victims is expected to steadily rise.

Going high-tech

The traditional tricks of "dumpster diving" or stealing wallets are being supplanted by high-tech methods. In the most advanced cases, hackers have penetrated databases and downloaded credit card numbers and other information.

Airman Armstrong's case was a low-tech job. However, in an October 1999 case, identity bandits hit more than 175 generals and admirals, stealing information via the Internet. The thieves used it to open almost 1,300 accounts — more than $1.4 million in credit.

A joint task force headed by the Secret Service

See **IDENTITY THEFT** Page 17

How high is your risk for identity theft?

Take this quiz to see how vulnerable you are to identity theft.

Each statement represents an avenue for an identity theft. If you agree with any of them, add the points to your score.

Quiz

You always carry your military identification card in your wallet (10 points)

Every week you receive several pre-approved credit offers (5 points; add 5 more if you don't shred them before tossing them)

You carry your Social Security card in your wallet (10 points)

You don't have a post office box or a locked, secured mailbox (5 points)

You drop off your outgoing mail at an open, unlocked box (10 points)

You don't shred or tear banking and credit information when you trash it (10 points)

You provide your Social Security card number whenever asked (10 points; add 5 more if you give it orally without checking to see who might be listening)

You're required to use your Social Security number as an employee number (5 points)

Your Social Security number is printed on an employee badge you wear (10 points)

Your Social Security number or driver's license number is printed on your checks (20 points)

You're listed in a Who's Who guide (5 points)

You carry your insurance card in your wallet, and it has your or your spouse's Social Security number (20 points)

You haven't ordered a copy of your credit report for at least two years (10 points)

You don't believe people would root around in your trash looking for credit information (10 points)

How vulnerable are you?

100-150: You're at a high risk. Get a paper shredder, become more security conscious and question why people need your personal data.

50-100: Your odds of being an identity theft victim are average, but higher if you have good credit.

0-50: You have a high security IQ. Don't let your guard down.

Source: Privacy Rights Clearinghouse/Utility Consumers Action Network

COMSEC requires proper use of secure voice products

By Master Sgt. James Charity
Information Assurance Office
Air Force Special Operations Command
Hurlburt Field, Fla.

The arrival of Future Narrow Band Digital Terminal secure voice products in the communications world brings with it a host of user security roles and responsibilities. FNBDT is a newly developed digital protocol embedded in the operational capability of many secure voice devices. FNBDT offers users state-of-the-art, high-speed voice and data transmissions far superior to existing legacy secure voice systems. As we begin phasing out existing legacy secure voice analog devices, such as STU-II/III, over the next few years, we'll see an emergence of updated FNBDT products, such as the desktop and tactical Secure Telephone Equipment, narrow band STE, and a host of other FNBDT cellular products.

As operators and communicators, we're always seeking to optimize mission capabilities with the latest and greatest available products. However, we too often charge ahead and overlook vital aspects of acquiring new technology. For example, what security risks are associated with using the product? Physical security? Emission security? Personnel security? Transmission security? Although these key concerns of COMSEC have existed for years, they're often considered last in the rush to "get the job done."

Many FNBDT products use personal identification numbers. Unlike the STU-III, which needs a crypto ignition key for secure operation, a PIN-activated secure phone requires an extra measure of physical security attentiveness and awareness to ensure communications security. A major risk with these devices is for users to leave them unattended with the PIN activated for short periods, such as while going to the restroom or on a smoke break. While activated, the device assumes the classification of the key, so leaving it unattended equates to leaving a classified document in the open for anyone to see. Needless to say, robust security measures are essential for proper use of these devices.

While each product has unique features, following the basic rule of familiarizing ourselves with its operating features will help prevent security incidents both in-garrison and deployed.

Local procedures for using and safeguarding these devices must be developed and periodically reviewed to ensure effectiveness. Units and users should contact their host wing COMSEC Office for specific guidance and information on purchasing and operating any new FNBDT product.

IDENTITY THEFT

From Page 16

caught the "slime-balls," but not before they ran up a $37,000 tab on 103 accounts.

These cases highlight one fact. Everyone is fair game for identity theft, including those in the military. Actually, most airmen are prime targets, because the military stresses financial responsibility, which usually translates into a good credit record. Someone with good credit is ideal for this new brand of thief, according to Cantrell.

But, there are actions you can take to lower your risk.

"Zealously guard your personal information," said Special Agent Bill Blaisdale, chief of OSI's nonviolent crimes branch.

Before providing personal information, find out how it will be used and if it will be shared. Pay attention to credit card billing cycles and follow up if bills don't arrive on time. Carry fewer identification and credit cards in your wallet or purse. Also, shred any pre-approved credit offers, bank statements and credit card billing information before discarding them.

"Thieves can make up to $30,000 a month doing this," Cantrell said. "For that kind of money, people will dig through trash. They'll break into your car. They're not even after your credit cards. They want your personal information."

The "beauty" of identity theft is most victims aren't even aware of the crime until it's too late. The average victim doesn't know they're a victim until some 14 months later.

To steal someone's identity all a person needs is a name, Social Security number, address and birthday. With that a thief can take over your financial accounts, open new accounts, apply for loans, buy a car or even rent an apartment.

Also, the penalties for identity theft aren't that harsh. In Airman Armstrong's case, his identity thief pled guilty to a laundry list of charges and is slated to spend just five years in the pokey.

Take action fast!

If you have your identity stolen there are three immediate steps to take.

First, contact the fraud departments of each of the three major credit bureaus (Equifax, Experian and Trans Union). Tell them to flag your file with a fraud alert. Next, contact creditors of any accounts that have been tampered with or opened fraudulently. Third, file a police report.

Airman Armstrong learned about identity theft the hard way, but he hopes other Air Force people can learn from his misfortune.

"If I try to write a check in a store, alarms start going off," Airman Armstrong said. "My credit is ruined, and I have to pay for everything in cash. Be aware of everything. Just because you're on a base don't assume you're safe."

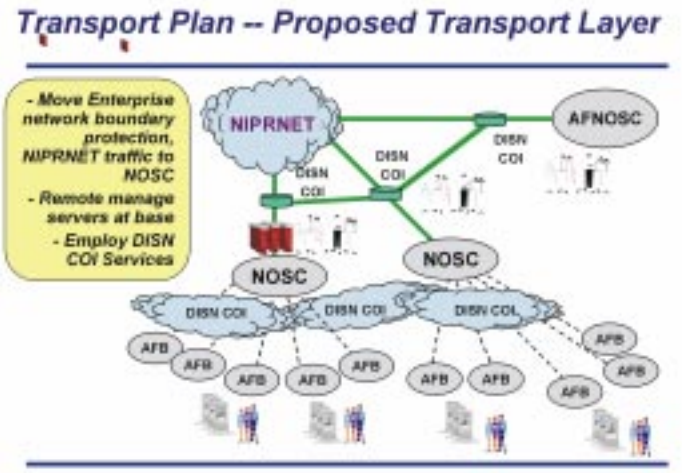
One Air Force … one Community of Interest network

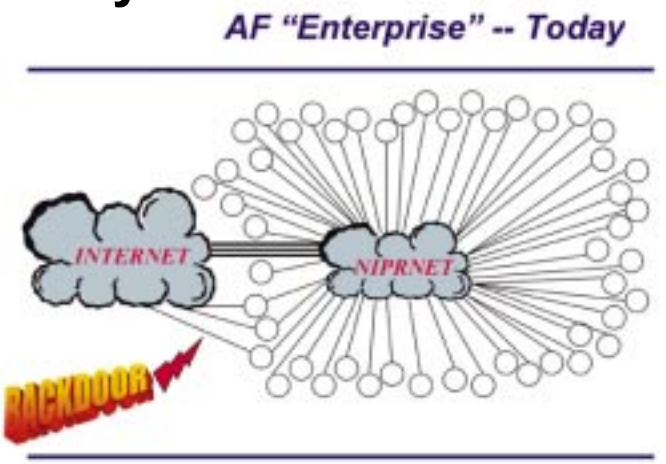
By Capt. John Anderson III
Base Networks Branch
Deputy Chief of Staff,
Communications and Information
Washington

So what exactly is the Air Force Community of Interest network? Simply put, it's the Air Force partnering with Defense Information Systems Agency to provide a highly secure, more robust, network "infostructure." The COI network establishes an "Air Force Intranet," which is a key enabler for several initiatives that began last summer with the Information Technology Summit indorsed by the Air Force chief of staff.

Today's environment is ideal for making necessary changes, based on a recent surge in network technology advancement, emergence of state of the practice information systems, and reduction in the cost of available bandwidth. By capitalizing on these advancements, we can match logical applications and network support services to a flexible architecture and improve overall system-wide efficiency. By enabling a tiered operational approach, the COI network will improve performance, increase overall network security, minimize latency, reduce costs, and posture Air Force communications for ease of continual change.

The COI network will be a net-centric enterprise framework of information transport services supporting all Air Force members at fixed bases, deployed locations, and on airborne platforms. The scope of the COI





network includes access to hundreds of active-duty Air Force, Guard and Reserve installations and facilities, and Air Force Recruiting sites. These access points require different amounts and types of communications and computing resources and services. The COI network gives the Air Force agility to strategically manage and operate the network for current and future requirements.

So why do we need a COI network? The Air Force shares a common network backbone with the Army, Navy and Marines, known as the Non-secure Internet Protocol Router Network. One of the primary concerns is the difficulty of managing the security of Air Force base networks within the largely unprotected NIPRNET environment. Since our networks have many internet access points and "back doors," security management challenges are increased.

Currently, Air Force wide-area design has hundreds of connections to the NIPRNET – one for each base and many geographically separated units. By implementing the COI network, we limit NIPRNET connections to MAJCOM Network Operations and Security Centers and greatly reduce security vulnerability.

While our current focus is high-speed, unclassified connectivity and security, our target is convergence of classified and unclassified base-level data, voice, video, imagery and telemetry requirements (multimedia). High-bandwidth wide-area service will move data quickly between Air Force operational locations and major processing nodes. Combined infrastructure installation of the Combat Information Transport System, Information Transport System, and Last 400' will provide capability to transport high-speed, multimedia, point-to-point or multicast information within the base environment and up to the access point to the wide-area transport networks – including NIPRNET, Secure

See **ONE AIR FORCE** Page 19

Roche sworn in as Secretary of the Air Force

TO THE MEN AND WOMEN OF THE UNITED STATES AIR FORCE

I was recently sworn in as your 20th Secretary of the Air Force and became, on that day, a proud member of a magnificent team of active duty airmen, guardsmen, reservists, and civilian employees. You have earned the admiration of our nation, the respect of the world, and the promise of a bright future. I already can tell you that you should be enormously proud of your achievements, from combat operations over Iraq and the Balkans to your recent validation of the Expeditionary Aerospace Force Concept. In the realm of aerospace power, you fly the best, train the best, and maintain the best. As you put it: "No One Comes Close."

Dr. James G. Roche

We must now turn our focus to the journey ahead, and be responsive to this new century's emerging security environment. I look forward to piloting that journey with you. My focus is on developing new strategies for military aerospace power in this new millennium; improving Air Force retention, professional education, and leadership development; eliminating the inefficiencies in how we do our business; and developing our acquisition policies and processes to ensure innovation and competitive vibrancy within our defense industrial base over the long haul. My vision is an aerospace future just as remarkable as your admired past: undeniable and global reconnaissance and strike superiority. My pledge to you is that I will serve the way you do every day, worldwide – with integrity, selflessness, and in earnest pursuit of excellence.

In 1963, President Kennedy said of military service: "I can imagine no more rewarding career. And any man who may be asked in this century what he did to make his life worthwhile, I think can respond with a good deal of pride and satisfaction: 'I served in the United States Navy.'" That sentiment rings very true for me. As you know, I am deeply proud of my Navy career. But, today we are in a new century, with new opportunities, new challenges, new capabilities, and vastly different threats to the security of our great nation. In this century, men and women can respond with a good deal of pride and satisfaction: "I serve in the United States Air Force." And now, I am proud to be able to say that too.

Dr. James G. Roche
Secretary of the Air Force

ONE AIR FORCE

From Page 18

Internet Protocol Router Network, Defense Information Systems Network, and asynchronous transfer mode services.

Our MAJCOM NOSC-centric construct will improve desktop data reliability by centralizing highly-skilled personnel, reducing the server footprint, increasing system up time, and minimizing span of control issues. By placing core service management at the NOSC level, base-level network control center personnel will be able to focus directly on touch labor support required to sustain information transport nodes, personal computers, and base-level servers. The Air Force Network Operations Center will continue to manage wide-area service delivery points and monitor DISA-provided wide-area connectivity.

The bottom line is an Air Force intranet makes sense! It gives the warfighter increased security and performance by leveraging our information technology resources as we strive to attain and maintain Information Superiority. We improve network performance and information security, and create centers of expertise at the MAJCOM NOSCs. With continued leaps forward in providing IT services, we'll ensure the Air Force realizes the CSAF's vision of *One Air Force…One Network*.

AF stands up network training centers: provides tools to operators, maintainers

By Master Sgt. Dave Mann
Air Force Communications Agency
Scott AFB, Ill.

The structured on-the-job training and Network Training Center initiatives are a big hit and, if SOJT's curriculum hasn't hit your base yet or an NTC hasn't already arrived, they're coming soon.

In fiscal 2000, 21 NTCs were fielded and 24 more so far in fiscal 2001.

SOJT is a process of providing needed network training to people charged with operating and maintaining our Air Force Enterprise Network. NTCs consist of a suite of networking equipment (routers, switches, workstations, server, testing tools, etc.) needed to provide a proper, hands-on network learning environment. These training centers are designed to provide a method to supplement C&I training received in technical school, facilitate skill level upgrades, sharpen the skills of "old timers" who haven't been to a technical school in a while, provide for any additional network training required by AEF tasked personnel, and give a protected environment to conduct necessary network task evaluations and qualification check rides.

John Marshall, Network Training Center instructor at Scott AFB, Ill., teaches subnetting from the first semester of the Cisco curriculum.

As with any new initiative, there are growing pains. While it's clear this training initiative is needed, appreciated, and put to good use, we're implementing improvements requested by career field managers and field units to shorten time needed to complete the training.

These requests, coupled with sharply rising program expenses, mandated a change in order to continue this worthwhile endeavor. After much research, a modified SOJT curricula delivery vehicle is soon to be put into effect. This modified process will retain full-time instructors at the MAJCOM NOSCs. It will also provide for centrally funded, certified, commercial training at base NTCs. The commercial training vendor will use the NTC where applicable, and provide instructors, any necessary training references, and additional required equipment to a NTC as scheduled by the MAJCOM. This training is what the commercial sector relies on for their training needs. Now our people will receive the most up-to-date and technically accurate certified training available—without the curricula development and maintenance tail.

Commercial training will include Windows 2000 Client Administration, Windows 2000 Server Administration, Networking Fundamentals, Networking Protocols, Internetworking with TCP/IP, and Internetwork Routing and Switching. This revised approach affords MAJCOMs the ability to sharpen the skills of a network professional through a more time-condensed program.

All this new training is the result of Air Force leadership's commitment to ensure professionalization of those who maintain a very crucial and valuable asset—the Air Force Enterprise Network. Leadership is committed to continuing scheduled implementation of the NTCs at each base with an Air Force Network Control Center. With the modified SOJT process, there's enough funding to expand fielding of NTC equipment beyond the original 88 locations and accelerate delivery so all remaining bases should have their NTC delivered no later than the end of calendar year 2001. All that remains is the continued commitment of commanders and supervisors to making the time for training.

Four Star Conference links senior AF leaders

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

The value of communications in today's military environment can't be overestimated. Seconds can mean the difference between winning and losing a conflict. As the top military member of the U.S. Air Force, Chief of Staff Gen. Michael E. Ryan needs a reliable real-time means to communicate with his commanders stationed around the globe. One valuable resource he uses is the Four Star Conference.

Connected over the Defense Red Switch Network, and built on a secure digital switch by members of the Air Force Pentagon Communications Agency, the Four Star Conference is the primary means for the chief of staff to talk to all Air Force senior leaders at the same time without being in the same location, said Col. Glenn F. Spears, executive officer to the chief of staff.

"These conferences are very important. They provide General Ryan an opportunity to speak to and interact with all of the Air Force's senior officials on a regular basis," Colonel Spears said. "In addition, they accommodate each of their busy schedules, since they don't have to physically be together."

With approximately 13 of the Air Force's top leaders on the phone at once, it's essential that the call be as productive as possible, with time being used effectively, Colonel Spears said. Conducted every six weeks, the conference usually lasts 30 to 50 minutes, depending on what's going on in the Air Force and the world.

"Topics run the gamut of Air Force issues, from people to force readiness and modernization," he said. "They talk about budget issues, operational tempo and making sure we continue to do the right things for Air Force people. The information shared and guidance given by the chief of staff is, at the strategic level for our Air Force, the same as an air tasking order to combat units, or movement orders for mobility units. It's key to the Air Force's continued success."

The sheer importance of the conference requires that it go off without a hitch. While on the surface it may seem like just another phone call, a lot of work goes on prior to, and during, the conference, ensuring participants stay connected and line clarity is maintained. Personnel in the Air Force Operations Center and AFPCA's switch maintenance branch combine their efforts behind the scenes.

AFOC members initiate the conference, ensuring all of the commanders are on the line. They also make sure the chief of staff and the secretary of the Air Force are aware of all Air Force operational issues, said Master Sgt. Sly Harris, AFOC Watch Operations superintendent.

"For the Four Star Conference, we follow the same concept as individuals working on an Air Force flight line," Sergeant Harris said. "While maintenance personnel in the Pentagon and MAJCOM communications centers make sure the phone lines (or jets) are operational, the AFOC executes and controls the phone call (or flight)."

While AFOC executes the call, members of the Air Force Pentagon Communications Agency switch maintenance branch are the executive agents who ensure the call happens. "We provide direction to support personnel in the Pentagon and around the world to pull off this conference," said Master Sgt. Ted Peters, AFPCA Command and Control Systems maintenance superintendent.

"For example, if a MAJCOM commander is traveling, we provide guidance to his staff to make sure he has access to at least two high-quality secure instruments. That's not always an easy feat. We deal directly with executive officers, switch maintainers, DISA and whoever else we need to make the conference perfect."

In order to guarantee perfection, AFPCA conducts a pre-conference two hours prior to the actual call. "Our primary purpose is to maintain the lines connecting principals into the conference," said Sergeant Peters. "A lot of people don't understand the importance of this Four Star Conference and ultimately the red switch. This is part of the tip of the spear when it comes to warfighting capabilities. During any major contingency, such as going to war or a nuclear attack, the red switch is the primary command and control instrument relaying this intention."

Of course maintaining the Air Force's premier communications tool comes with certain expectations. "General Ryan expects the system to work 100 percent of the time – national security depends on it," Sergeant Peters said. "That's why these Four Star Conferences are so important. They not only serve as a way to relay important messages throughout the Air Force on a regular basis, but they also ensure the system works."

Due to the importance of the conference, a rehearsal is held a few days in advance. This practice session is conducted by AFPCA, AFOC, the chief of staff's executive officer and players appointed by the principal commanders, and serves to work out all of the bugs before the "real" phone call.

"We know when there's a problem," Sergeant Peters said. "If a red phone unplugs from the system, we get an audible alarm and a printout. But the key is ensuring problems are worked out before the conference. The network pipeline consists of a lot of cables, people and circuits, so troubleshooting and pinpointing problems can take some time. We can't afford to have a

See **4 STAR CONFERENCE** Page 23

Specialty programs available to career registrants

RANDOLPH AIR FORCE BASE, Texas – The Communications and Information Career Program supports over 10,000 registrants and offers career counseling and competitive job opportunities to Air Force employees working in communications, computers, information management and visual information. It also offers hiring assistance (i.e., candidate referral list, career briefs, and selection guidance) to military and civilian supervisors filling career program positions. Additionally, it administers the following specialty programs:

Civilian Competitive Development Program

CCDP is part of a larger framework for developing civilian leaders. The program includes in-residence Professional Military Education, long-term academic and experiential programs and short-term executive programs. All are included in one of the following schools or programs:

- Intermediate Service School – Air Command and Staff College
- Senior Service School – Air War College
- Academic and experiential programs
- Executive development programs

Note that ACSC and AWC can be completed in-residence, by correspondence or by seminar. Check with your local education office for details.

All employees, including career program registrants and non-career program registrants, who meet the eligibility criteria, will be considered for Air Force-wide competition. Please note that while this process is managed by the career programs, a separate call for CCDP goes out annually for nominations.

Defense Leadership and Management Program

DLAMP is a systematic program of joint civilian leadership training, education and development throughout the Department of Defense. It provides a framework for developing civilian leaders with a DOD-wide capability for approximately 3,000 key positions. In addition, DLAMP promotes shared understanding and mission sense among civilian and military personnel. DLAMP is open to Air Force employees in grades GS/GM-13/14/15.

Career Broadening

CICP career broadening opportunities provide developmental experience for new skills in the communications and information functional arena; broaden existing functional skills; and enhance leadership perspectives. We announce requests for host sites and applicants periodically throughout the year. Announcements for career broadening applications are posted on our Web site, so monitor it frequently to ensure you don't miss opportunities.

Assignment to a career broadening position is limited to 24 months (with management extensions up to 36 months), and may involve a temporary promotion. Selectees must sign an Air Force-wide mobility statement.

Training and Tuition Assistance

CICP offers managerial development and training focusing on technical management, professional development and executive development. This is accomplished through short- and long-term training, management and executive seminars, and self-improvement activities. Using the Air Force Civilian Career Programs Training and Development Guide, registrants should list the types of training desired in their annual Career Enhancement Plan. The CEP, normally filled out in the March-April timeframe, is CICP's main source for determining training requirements.

CICP registrants may request funding support through the CICP Tuition Assistance Program, if they're in a covered position or a member of the CICP feeder group, and are pursuing a communications and information-related undergraduate or graduate degree. Tuition assistance is offered on a "funds available" basis; we currently pay 75 percent of tuition. Application packages can be downloaded from our Web site. Submission deadlines are July 1 and Dec. 1, but acquisition position registrants may apply at any time.

Palace Acquire Intern Program

The Palace Acquire Intern Program is a civilian workforce renewal effort funded by Headquarters Air Force and administered by the Air Force Personnel Center. The program targets college graduates and offers two-to-three years of formal and on-the-job training at Air Force organizations throughout the continental United States Communications and information PAQ positions include communications-computer systems specialists, computer scientists, operations research analysts, and electronic/computer engineers. Organizations interested in sponsoring a PAQ intern and prospective applicants may contact us for more information.

How to Register in CICP

Air Force employees who possess the appropriate grade and skill codes may register in the CICP. To determine if you're eligible, visit your local CPF or our Web site. To register, complete an AF Form 2675, Civilian Career Program Registration and Geographic Availability, on line or submit it to your local CPF.

Visit the CICP Web Site

The CICP Web site contains a wealth of information for registrants. Visit it at http://www.afpc.randolph.af.mil/cp/cicp.

AEF Center offers new Web format

By Lt. Col. Bryan A. Holt
Aerospace Expeditionary Force Center
Langley AFB, Va.

The Air Force's Web-based deployment tool, EAF Online, has been redesigned to give airmen more help with Aerospace Expeditionary Force issues.

The Aerospace Expeditionary Force Center revised the Web site to provide more information, enhanced access and the convenience of a single source for all AEF deployment information. The center is the agency for implementing the Air Force's Expeditionary Aerospace Force concept.

"This is a major milestone to provide better service to those deploying," said Lt. Col. Marie Barboza, AEF Center project officer for EAF Online.

The new format combines features of the previous AEFC site into a Web "portal," which provides access to various databases and can be customized for each user. The site offers an array of information, including deployment checklists, the AEF Commander's Playbook, lessons learned, and the newest feature, the Commander's Toolkit.

The major attraction for deployers is the position descriptions containing information on the duties, requirements and conditions of specific deployed positions. Users get the information by first registering at the site, which establishes their profile. Subsequent logins provide information tailored to the user's career field.

The deployment checklist includes training, medical status and other qualifications required for deployment, as well as links to references. Commanders can track training requirements of their people.

The Commander's Toolkit upgrade to EAF Online allows commanders to track the deployment status of their unit and people. Future enhancements will include a training module to track skill level training and a module to track operations tempo. All modules are updated by pulling data from existing Air Force sources, such as the Personnel Data System.

"EAF Online is also very beneficial to Air Force Reserve and Air National Guard members," Colonel Barboza said. The position descriptions and the Commander's Toolkit include information for active, Guard and Reserve personnel.

The restricted Web site can be accessed via military and government computers at https://aefcenter.acc.af.mil/. The AEFC has also added a public Web site accessible from any computer through EAF Online or http://aefc.langley.af.mil. Updated daily, the unclassified site allows users to link to EAF/AEF activities, theater information and other key issues.

"As the AEF construct matures, the unclassified Web site provides critical information to the general public, family members and news media representatives on how the Air Force conducts business in the 21st century," Colonel Barboza said. "This also allows Air Force people to get certain AEF information from their home computer."

The sites offer "one-stop shopping" for anyone eligible to deploy or wanting more information about the EAF concept and AEF process. EAF Online also gives individuals an opportunity to provide feedback.

"It's critical that everyone identified for an AEF go to EAF Online to obtain the latest information they need for their deployment," Colonel Barboza said. (AFPN)

---

4 STAR CONFERENCE

From Page 21

problem during the real deal.

"Perfection is the standard," Sergeant Peters continued. "We (AFPCA) go a mile beyond what people generally expect out of a communications or maintenance organization. We have to get to everything right now, because that's the expectation of our customer – that's the service we try to provide."

The intense preparation seems to pay off. "I've been involved with Four Star Conferences for almost a year and, knock on wood, each one has gone very well," Colonel Spears said. "That doesn't mean that while the four-star generals see the duck floating smoothly on the water, there's not a lot of paddling going on under the surface – I know there is. General Ryan appreciates the work of the literally hundreds of folks behind the scenes who ensure the conferences are successful and smooth.

"What does that success mean? It's more than just a regular phone call," Colonel Spears said. "It maximizes time for these senior leaders to communicate and to assure our Air Force is being led in one direction. It's the whole team working behind the scenes who make it happen."

Center validates improved warfighting capabilities

By Capt. Todd Fleming
Public Affairs
Aerospace Command and Control, Intelligence, Surveillance and Reconnaissance Center
Langley AFB, Va.

The Combined Aerospace Operations Center-Experimental here has proven its worth, according to Air Force officials. The center recently completed an operational assessment that will result in delivery of command and control hardware and software with innovative and expanded capabilities to the new CAOC at Prince Sultan AB in Southwest Asia.

"The system is working very well," said Lt. Col. Randy Lefevre, Central Air Forces. "We're ensuring the process works end-to-end and we're fine-tuning it. CAOC-X is a phenomenal test bed and tool to bring out this command and control system."

A CAOC is the primary theater command and control facility responsible for orchestrating an air campaign for a coalition effort. Prince Sultan's CAOC is responsible for overseeing enforcement of the no-fly zone over Iraq.

CAOC-X was established by Air Combat Command and Air Force Materiel Command to help operators, acquisition professionals, testers and industry experts quickly deliver newest technologies and processes to aerospace operations centers through a process called spiral development, said Col. Craig Lightfoot, CAOC-X director.

CAOC-X represents a new paradigm in Air Force thinking that recognizes the need for quicker delivery of the latest technology, particularly in the area of information technology, Colonel Lightfoot said.

Much of the effort of CAOC-X is focused on turning the AOCs into a standardized weapon system that has a professional core of C2 operators, and current and standardized technology and processes. The Air Force is focused on creating expeditionary CAOCs that have a small footprint in terms of hardware and personnel, employ certified operators, and provide decision-quality, actionable information that enables the commander and his staff to command aerospace power.

Currently, all of the AOCs around the world have different configurations. The goal is to standardize them into a single weapon system configuration, allowing for some minor variations based on mission needs.

"Although now a hub for bringing in good ideas, CAOC-X will ultimately serve as a prototype for all AOCs," said Col. Pete Hoene, Electronic Systems Center. "It's both a development and assessment tool.

"While short-term exercises and experiments help decision-makers determine what works well and what areas need improvement, the ability to rapidly develop, and realistically test, promising initiatives is essential to realizing the true vision of the AOC weapon system," he said.

The successful operational assessment completed by the CAOC-X is a prime example.

"We've been doing an evaluation to ensure the necessary information can be integrated and passed over networks," said Dennis Yaskowsky, Theater Battle Management Core System senior analyst. "The operational assessment will take data and evaluate how the information will support the warfighter in terms of speed of service, data reliability, and executable efforts.

"By April, we're going to deliver the Block 10 baseline, the initial configuration required to establish Prince Sultan's use of the CAOC," he said.

The Block 10 baseline is the first series of capabilities that will be delivered to AOCs throughout the Air Force. Additional capabilities will be added and further developed in future "block" deliveries, in a manner similar to how other weapons systems are currently upgraded.

The TBMCS is the suite of command and control software required to orchestrate aerospace operations. It consists of many systems integrated into a complete battle information system.

Features being delivered in the Block 10 baseline include giving coalition forces a releasable air tasking order, and a 24-hour plan to execute air operations. It also creates an air picture of battlespace that shows where all aerospace assets are located at a given time that can be released to other coalition nations. The system also disseminates releasable intelligence products, and reduces the hardware footprint in an open coalition environment, meaning cutting back significantly on equipment required in a CAOC.

"We identified several hardware, software and process issues that we worked through cooperatively to provide the best solution to the field," said William Merrill, CAOC-X systems manager from ESC. "Had we not done this here, we would have discovered these issues at Prince Sultan and been forced to work through them on the spot with a lot less support and within the time constraint pressures of standing up a new overseas facility."

"The bottom line," Yaskowsky said, "is getting the systems to operators in the field in minimum time."

In addition to the AC2ISRC and the Electronic Systems Center, the CAOC-X team has participants from ACC's Aerospace Operations, and Communications and Information Systems directorates, 8th and 9th Air Forces, Air Force Research Laboratory, Air Force Operational Test and Evaluation Center, Command and Control Battlelab, 46th and 605th Test Squadrons, 609th Air Communications Squadron, Air Mobility Command, the Command and Control Theater Innovation

See **CAOC** Page 28

Air Force developing C2 'constellation'

LANGLEY AIR FORCE BASE, Va. – The Air Force held its first industry day for the Multi-Sensor Command and Control Constellation in May at Langley, in conjunction with the National Defense Industrial Association. The conference hosted about 260 military and industry representatives.

MC2C is a future "constellation" of air and space command and control, intelligence, surveillance and reconnaissance capabilities – consisting of space-based systems, unmanned aerial vehicles, ground stations, and possibly a new multi-sensor command and control aircraft to replace the existing array of C2ISR aircraft.

"It's critical that we develop machine-to-machine interfaces that allow all our C2 and ISR assets to pass information seamlessly to whoever needs it," said Maj. Gen. Jerry Perryman, Aerospace C2 and ISR Center commander. "Many of our assets are stove-piped, meaning that they only talk to their processing stations. We need them to be horizontally integrated in this constellation so they can communicate across the spectrum and ensure decision-quality information is delivered to our commanders."

"This may mean that we'll need a new multi-sensor command and control aircraft as part of the constellation, or that we'll need to upgrade current systems with new technology that enables these machine-to-machine interfaces. We're working aggressively to identify the best option for making this constellation as effective as possible," he added.

One possibility under consideration is to migrate capabilities currently delivered by AWACS, Joint STARS, Compass Call, Rivet Joint, U-2, and Airborne Command and Control Center, to a new multi-sensor command and control aircraft that could be configured for different missions, and a constellation of high- and low-altitude unmanned aerial vehicles.

This – coupled with improvements in space-based systems, perhaps the most important component of the constellation – would significantly increase warfighting capability, said Col. Wilson Guilbeaux, MC2C team lead from the Aerospace C2 and ISR Center.

"This effort presents an opportunity to develop enterprise management techniques applicable to complex system-of-systems programs," said Col. Gary Connor, MC2C team lead from the Electronics Systems Center. "That means doing whatever it takes to break down stove-piped barriers of individual systems, and focusing on battlefield effects our users need to achieve operational objectives."

Focusing on these effects is a matter of "beginning with the end in mind" and developing a set of integrated capabilities that allow the warfighter to achieve that end, that required battlefield effect, the colonel said.

Adding a multi-sensor C2 aircraft that can be configured for different missions to the constellation would help mitigate long-term platform sustainment issues, according to Lt. Col. Rob Whitaker, from the Aerospace C2 and ISR Center's Sensors and Platforms Division.

"Current C2 and ISR aircraft are primarily based on the aging Boeing 707/C-135 and C-130 aircraft," said Colonel Whitaker. "Sustaining the E-3 AWACS, E-8C Joint STARS, variants of the RC-135, EC-130, Compass Call, and EC-130 ABCCC, are costly due to decreasing reliability and maintainability, vanishing vendor items, and aging airframes."

Space is viewed as an increasingly critical component of the new constellation, with development of space-based infrared and space-based radar.

"Space is an important aspect of MC2C because it will provide persistent, worldwide, on-demand surveillance and reconnaissance for battlespace characterization, mission planning, execution and assessment," said 2nd Lt. Ron Killins, Aeronautical Systems Center.

"Integration of space and air systems in a collaborative approach will provide users a responsive, continuous, multi-theater capability to detect, identify and track air and surface objects, regardless of their motion or location, and weather conditions," added Maj. Jim Passaro, Air Force Space Command.

"... I believe our team will keep its focus – how best to integrate air and space C2 and ISR capabilities to deliver the greatest capability to our warfighters."

MC2C is an integral component of the Air Force's Global Strike Task Force, which will combine stealth and advanced weapons with an integrated C2ISR system. Supported by MC2C, B-2s and F-22s will deliver the first blows to enemy threats. Gen. John P. Jumper, Air Combat Command commander, envisions the Global Strike Task Force as a "kick down the door" force providing access to battlespace in the 21st century.

"These integrated capabilities would focus on achieving desired operational effects, enabling the GSTF to prevail across the spectrum of pre-conflict and conflict scenarios," said Colonel Connor.

"This complex task of creating the MC2C will require an aggressive total-team effort," said General Perryman.

Industry went to Langley to help the government develop and refine acquisition strategy, and leverage industry's investments into systems engineering, analysis, and simulation-based acquisition tools.

"Now that we've engaged industry, our team enters a new and more demanding phase of activity this summer," said Colonel Connor. "Our dialogue with industry will increase tenfold, helping us to shape concepts and focus on the right questions to answer. But in the end, I believe our team will keep its focus – how best to integrate air and space C2 and ISR capabilities to deliver the greatest capability to our warfighters."

Fairchild runway relocation: a communicator's perspective

By Maj. Jeffrey Kromer
92nd Communications Squadron Commander
Fairchild AFB, Wash.

"As good as Fairchild's." That was the number one planning objective used to determine the desired level of communications and information service to be provided from May to mid-August to members of the 92nd Air Refueling Wing deployed to March ARB, Calif. With Fairchild's runway undergoing major refurbishment, the wing chose March for its base of operations during the summer closure. This Total Force effort proved to be a rich experience in providing deployed communications and information support.

A cross-functional wing working group met weekly for six months to plan every aspect of the deployment. For the 92nd Communications Squadron, planning included the full range of communications and information media to ensure service was "as good as Fairchild's." To Capt. Mike Moyles, 92nd CS Mission Flight commander, and his staff, that meant planning for telephones, ground-to-air radios, land mobile radios, official and private mail delivery, cell phones, pagers, and full Fairchild Metropolitan Area Network connectivity – each to the same high level of customer satisfaction Team Fairchild members were accustomed to at home base.

Even though the deployment was to a CONUS location, planning mirrored that for deploying to an overseas bare base. As with any deployment, the questions are the same, only the implementation varies. Tech. Sgt. Carlos Gonzalez led the communications and information team. The 452nd CS was a gracious host and the two units formed a true Total Force team to solve many devil-in-the-details challenges.

Some connectivity was fairly straightforward, with 50 telephone lines extended from the base telephone switch to the 92nd ARW's temporary building, and further extended to the work areas by Staff Sgt.Ralph Basilio and Airman 1st Class Ron Green. Other connectivity proved much more perplexing. Staff Sgts. Matt MacDougall and Matt Green first had to obtain special permissions to mount temporary ground-to-air radios on historically protected buildings. The 92nd CS integrated its new narrow-band land mobile radios into the 452nd ARW flight line nets. The March ARB post office set up a temporary general delivery address for official and private mail delivery. Airman 1st Class Samantha Pedersen, deployed information manager, became a one-person postmaster, picking up and delivering incoming and outgoing daily mail. Fairchild leadership had become quite used to their home-base Nextel cellular phones. Their unique private and group push-to-talk modes emulated command radio nets without using scarce military frequencies. These phones were reprogrammed to the March ARB area and new push-to-talk groups created to mirror the deployed organizational structure. Seventy-five commercial pagers were locally leased, giving coverage to the southern California area.

Photos by Staff Sergeant Dominic Hauser

Airman 1st Class Ronald Green, 92nd CS, patches telephone lines from March ARB's telephone network into the demarcation box to give the deployed 92nd ARW telephone connectivity.

A unique aspect of the deployment was the solution developed to give operations access to the Fairchild Metropolitan Area Network that was "as good as Fairchild's." It was conceived by 92nd CS network team members Tech. Sgt. Elaine Farver, and Airmen 1st Class Steve Rowe, Brian Menenga, Michael Schultz, Adam Letourneau and Matt Mattoon. A common approach to this challenge is to incorporate deployed forces into the existing host MAN. However,

this would have required the host NCC to create and administer 390 new accounts, after first installing new infrastructure and hiring additional temporary staff to accommodate the additional users. This approach would have caused deployed personnel to lose easy access to files and computer programs stored on Fairchild servers. The solution was borrowed from Air Mobility Command's Command and Control Information Processing System, which uses a Virtual Private Network to link AMC bases into a common network.

To provide Fairchild LAN connectivity at March, it was decided to implement a Windows 2000 VPN, which enabled remote access to the Fairchild network equivalent to being directly connected back at home base. Regular logons were used to access e-mail, shared drives, application servers and the intranet. The only requirement for running this type of VPN was to have two servers, one at each end running Win2K, with routing and remote-access features enabled, and an internet connection.

VPN provides secure communications across the internet using the Layer 2 Tunneling Protocol, and IPSec, a commercial packet encryption scheme. L2TP hides all internet protocol addresses on both sides of the connection by forming a tunnel using the servers' IP addresses. When a packet comes into the server, the entire packet – including transfer control protocol headers of the destination and source IP addresses, server ports and message payload – becomes the payload of a new host packet. The host packet "tunnels" through the internet between the two VPN server external subnets. Base network firewalls at each end of the VPN path need only one port opened to allow VPN host packets to pass through to base MAN internal subnets. As host packets are passed through VPN servers from the external subnet to the internal subnet, the WIN 2000 software strips off host packet headers, revealing internal subnet IP addresses of the original packets. At that point, packets look identical to other packets generated within the subnet and get routed to their intended destination as normal network traffic.

IPSec protects packets as they traverse the internet tunnel. Within VPN servers, the entire payload is encrypted, leaving only the host IP address and firewall port assignments in the clear for routing. IPSec uses mutual authentication to validate both ends of the VPN connection with "kerberos," or certificates. Additional protection is provided against packet alteration through a secure hashing algorithm that detects data changes inadvertently introduced during transmission.

Using a dedicated server for VPN provides tighter security, eliminates the need for additional configuration of individual clients at the desktop, and gives full range access and functionality. L2TP and IPSec run transparently to the client, allowing it to function with all network services that don't run their own encryption. Is it really "as good as Fairchild's?" As with all new systems, there were growing pains. The deployers

Airman 1st Class Matthew Mattoon, 92nd CS, strips wire to create a local area network cable.

haven't successfully passed C2IPS traffic through the VPN. This may be due to conflicts between encryption schemes used by each VPN. As a workaround, C2IPS workstations ran on static assigned IPs in parallel with the VPN subnet. By far, the biggest hindrance to efficient operation of the VPN is the limited internet connection speed at each base. The single T-1, or 1.544 MB/s "pipe," used for all internet traffic at each base becomes the system choke point. This path proved too slow to allow effective data transfer between our VPN and remote databases at Tinker AFB and Maxwell AFB Gunter Annex for Standard Base Supply System and GO-81 systems. These workstations were moved to independent subnets to optimize performance. Network analysis of traffic and control flow is helping to minimize effects of these choke points.

The 92nd ARW relocation to March has been a watershed of lessons learned for the 92nd CS "King Commers." This summer the 92nd CS will receive new deployable network capability through the Theater Deployable Communications Integrated Communications Access Package. It's anxious to explore concepts of using VPN technologies in future deployed networks supporting the AEF, Lead Mobility Wing, and Tanker Strategic Aircraft Reconstitution Team. Future deployments will demand transparent access to home networks. Given enough bandwidth, VPN technologies may be the avenue to provide much of this capability.

Mentoring goes virtual with eVector

By Senior Airman Matthew Miller
Air Force Personnel Center News Service
Randolph AFB, Texas

Commanders and supervisors now have a quick and easy way to track their officers through Air Force Personnel Center's newest online mentoring tool: eVector.

Much more than the typical "single uniform retrieval format" document currently available on each officer, eVector provides valuable information on other topics, such as military pay and per diem, service dates, promotion eligibility, decorations, joint and rated information. The eVector format includes career progression guidance, education and training information, assignment preferences and duty history.

"Our culture requires mentorship at many levels, but particularly at the commander level," said Lt. Gen. Donald Peterson, Air Force Personnel deputy chief of staff. "As an example, our Air Force assignment system mandates commander involvement and mentoring. Since we require our folks to mentor their people, we needed to provide a user-friendly mentoring tool for them. The answer was eVector. Mentoring is important to our Air Force. It positively impacts retention and allows for more effective use of our resources."

"eVector pulls everything together in one place," said Lt. Col. Mike Gamble, Air Force Personnel assignment programs and procedures division chief. "It includes information specific to the individual, and links to programs and resources a mentor might want to refer to when counseling."

More than 30 links to other career-related Web sites, such as tuition assistance programs, relocation information, Air Force Aid and GI Bill, are available with eVector.

A mentor can use the data to give accurate advice tuned to the individual's needs and circumstances, Colonel Gamble said.

"We wanted to capitalize on the information already available in the assignment management system and the AFPC home page, and consolidate links to other important career-related Web sites," Colonel Gamble said. With eVector, individuals can access a large amount of information on themselves, and easily grant permission to others whom they consider "mentors," all in one convenient location.

Permission will automatically be given to the officer's preference worksheet reviewer, most often the unit commander. Other access must originate from the member.

"With this feature, individuals control who sees their information," Colonel Gamble said. "They can designate several mentors, including those outside their chain of command. We realize that your 'mentor' may be someone at another base, and eVector facilitates that relationship. Of course, we encourage all officers to grant access to their current supervisor, as well as the person who has the most influence on their career. Current capabilities do not allow AFPC to automatically grant access to supervisors. However, we expect to include this function in future enhancements."

"A similar version of eVector is currently under development for our enlisted members," said 1st Lt. Joe Golembiewski, Air Force Personnel assignment systems program development officer. It will provide basically the same information to their mentors, plus information unique to enlisted members.

In the meantime, there is an enlisted page that offers links to several enlisted career-related Web sites.

Individuals can access eVector through the assignment management system, a secure network connection on the AFPC home page at http://afas.afpc.randolph.af.mil/afas/afas-main1.htm. (Courtesy of AFPC News Service)

CAOC

From Page 24

Group, and Air Force Special Operations Command.

The organization also relies on key companies in the information technology and defense industries.

"This has been an outstanding team effort from all the organizations and communities working together as a team to mitigate risks, thereby ensuring the best C2 system is fielded at PSAB in support of Joint Task Force-Southwest Asia," said William Diemand, 605th Test Squadron.

"After plenty of growing pains, we've put together the A-team and charted a course many thought was impossible," said Capt. Tony Perkins, CAOC-X chief of communications information. "It normally takes about two years to move an AOC, based on civil engineering, communications, operations, and testing and assessment requirements. We're doing it in nine months." (AFPN)

System administrators are not criminal investigators

By Joseph J. Hinds
Office of the Chief Counsel
Air Force Communications Agency
Scott AFB, Ill.

Staff Sgt. Ima Server, a systems administrator in the Network Defense section of the Communications Squadron at Globalcom AFB, was reviewing the proxy server logs one morning as the sun squeezed through his office blinds, showing the slowly rising steam from his coffee cup. Sergeant Server glanced at the calendar, noting that it was Friday the 13th, so he resolved to be careful.

As he was examining the proxy server logs, he noticed a large number of hits on Kiddiesex.Com, a known child pornography site. The hits were coming from a specific computer that was accessing the site many times during the week. Sergeant Server knew that Kiddiesex.Com was not an official business site. Also, the hits were too frequent and too long in duration to be inadvertent or accidental.

Furthermore, he remembered part of a system administrator's monitoring responsibilities included reporting improper internet use; once suspected system abuse was discovered, he had a duty to report it to his supervisor. His boss would then report it to the appropriate investigative authority or commander – in this case, the Air Force Office of Special Investigations. Sergeant Server also remembered being briefed that he wasn't a deputized criminal investigator and he shouldn't go beyond this point on his own, even though a "consent to monitoring" banner popped up each time a user turned on a computer. He knew he should report abuse of the system like a doctor reports child abuse, but he shouldn't probe the system on his own for the sole purpose of looking for additional evidence of the misuse.

In this hypothetical situation, child pornography was the subject matter of the abuse, but it also could be use of auction, gambling or other non-official business sites.

He next contacted lawyers at the Air Force Communications Agency Legal Office to ensure his actions were appropriate. Sergeant Server beamed as the cyber attorney praised him for thinking before leaping. He had stopped at the proper point before turning his monitoring activity into an illegal investigation and had contacted AFOSI immediately. The AFCA lawyer also advised him his local base SJA would assist him if this evolved into an investigation.

The Electronic Communications Privacy Act sets restrictions on how far Sergeant Server can go when protecting the network. His awareness of rules governing proper monitoring activity alerted him to the need to report this activity and get guidance from his local JA. The consequences for violating this particular law could lead to his imprisonment for up to five years … not a good thing. The law does contain the service-provider exception, but penalties for being wrong also require that he be aware of its limitations.

The system administrator is an employee of the service provider, in this case the Air Force, and may protect the rights of the service provider's property. However, as a general rule, these employees, on their own, may not cross the line into the investigation arena. There's a temptation to go after bad people who abuse government networks and put them behind bars, but this is beyond the scope of the system administrator's authority and job.

The Department of Justice's Search and Seizure Guide instructs law enforcement officials not to ask or direct a system administrator to monitor for law enforcement purposes without a Title III court order, issued when it's shown there's probable cause to believe a crime has been committed. In the Air Force, AFOSI usually uses an AFOSI Form 52, generally approved by the AFOSI commander, which is also issued based on probable cause.

In this case, the discovery that an Air Force member was accessing apparent child pornography would probably form the basis for probable cause. But he could go no further until the actual warrant or authorization was issued and then only under direction of the appropriate law enforcement authority.

There's a difference between monitoring for protection of property and monitoring during a criminal investigation. To stay within proper bounds, use the team approach. Check with your supervisor, base law office or OSI detachment, or AFCA/JA, at DSN 779-6060, for assistance. Information protection is everyone's responsibility.

Promotions

Captain
Patrick J. Swackhammer
AFCA, Scott AFB, Ill.
Andrea Moore
AU/SC
Maxwell AFB, Ala.

Technical Sergeant
Blaine Bish
Travis Stroup
Robert Robertson
3rd CS, Elmendorf AFB, Alaska

Senior Airman
Greg Gustafson
Dustin Howard
Leigh Samons
Colleen Ceniceros
Gabriel Perez
Lacashana Knight
3rd CS, Elmendorf AFB

Airman 1st Class
Franklin Guerrero
3rd CS, Elmendorf AFB

Awards

Civilian of the Quarter
Ruby Johnson
355th CS, Davis-Monthan AFB, Ariz.
Ramona L. Shannon, Category I
Andrew Dickey, Category II
3rd CS, Elmendorf AFB
Barbara Lowe
375th CSS, Scott AFB

Company Grade Officer of the Quarter
2nd Lt. Gilbert Hinojosa
355th CS, Davis-Monthan AFB
2nd Lt. Ryan Combs
3rd CS, Elmendorf AFB
2nd Lt. Dennis J. Daniels
375th CSS, Scott AFB

Senior NCO of the Quarter
MSgt. Joseph Jackson
355th CS, Davis-Monthan AFB
SMSgt. William Miranda
3rd CS, Elmendorf AFB
MSgt. Ray G. Anderson
375th CSS, Scott AFB

NCO of the Quarter
SSgt. Jonathon Woody
355th CS, Davis-Monthan AFB
TSgt. LeAnn Hugeback
3rd CS, Elmendorf AFB
TSgt. Michael Rodriguez
375th CSS, Scott AFB

Airman of the Quarter
A1C Kaniela Denis
355th CS, Davis-Monthan AFB
A1C Daniel Peden
3rd CS, Elmendorf AFB
SrA. Brent A. Poff
375th CSS, Scott AFB

Distinguished Graduate
MSgt. Pamela Matthews
Senior NCO Academy, Davis-Monthan AFB
SSgt. Shawnetta Jordan
Airman Leadership School, Davis-Monthan AFB

Levitow Award winner
SrA. Nicole Jirik
Airman Leadership School, Davis-Monthan AFB

Graduated Airman Leadership School
SrA. Angel Tellez,
Davis-Monthan AFB

Medals

Meritorious Service Medal
Maj. Jose Diaz (2OLC)
AU/SC
Maxwell AFB, Ala.
MSgt. Thomas Ewenson
AU/SC
Maxwell AFB

Valor & Recognition

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

ABS	Air Base Squadron
ACOMS	Air Communications Squadron
AFCA	Air Force Communications Agency
AFIAA	AF Intelligence Analysis Agency
AFFMA	AF Frequency Management Agency
AFCQMI	AF Center for Quality and Management Innovation
AFPCA	AF Pentagon Communications Agency
AFSOC	AF Special Operations Command
AFTAC	AF Technical Applications Center
AFWA	Air Force Weather Agency
ASOS	Air Support Operations Squadron
CCS	Combat Communications Squadron
CG/Comm Gp	Communications Group
CLSS	Computer Logistics Support Squadron
CS	Communications Squadron
CSG	Computer Systems Group
CSO	Computer Support Office
CPSS or CSS	Computer Systems Squadron
DISA	Defense Information Systems Agency
EIG	Engineering Installation Group
EIS	Electronics/Engineering Installation Squadron
IOG	Information Operations Group
JCSE	Joint Communications Support Element
MSG	Materiel Systems Group
RSG	Regional Support Group
SSG	Standard Systems Group

MSgt. John McCormick
3rd CS, Elmendorf AFB
MSgt. Kenny Quinn
509th CS, Whiteman AFB, Mo.

Joint Service Commendation Medal

Capt. Gerald Stewart
A1C Robert Milligan
3rd CS, Elmendorf AFB

Air Force Commendation Medal

TSgt. Terry Miracle
TSgt. Robert Miller
TSgt. Terrence Winn
SSgt. Anthony Mixon
SSgt. Philleas Phillps
SSgt. Brian Studinski
3rd CS, Elmendorf AFB
SSgt. Shannon McCann
SSgt. Duane Keil
509th CS, Whiteman AFB

Air Force Achievement Medal

TSgt. Daryle G. Christensen
SrA. Kristoffer E. Helfert
SrA. Daniel R. Krantz
SrA. Robert J. Kranz
509th CS, Whiteman AFB
CMSgt. Bud Butterfield (1OLC)
SMSgt. Joe Grindel (1OLC)
MSgt. Tim Colfer (1OLC)
MSgt. Ray Vintinner (1OLC)
TSgt. Brian Smith (2OLC)
TSgt. Jack Decker (1OLC)
TSgt. Chris Hillman (1OLC)
TSgt. Tim Sinclair (1OLC)
TSgt. Curt Worster
SSgt. Mark Giles
SSgt. Josh Hunsinger (1OLC)
SSgt. Dennis Grivois (1OLC)
SSgt. Kim Petry (1OLC)
SrA. Tony McPherson
101st Communications Flight
Bangor, Maine
SSgt. Robert Davis
SSgt. David Delozier
SrA. Earl Mollenido
SrA. Frank Robinson
3rd CS, Elmendorf AFB
A1C Mario Delos Santos
A1C Anthony Ferreira
509th CS, Whiteman AFB
Capt. Patrick J. Swackhammer
AFCA, Scott AFB

AACS Alumni Association plans reunion

By Chief Master Sgt. Richard P. "Hank" Sauer (USAF, Ret)
Executive Director
AACS Alumni Association

The AACS Alumni Association will hold its 25th annual reunion Sept. 20-23 at the Knoxville Hilton, Knoxville, Tenn. The association is comprised of former Air Force personnel who served in any capacity in any Army Airways Communications System, Airways and Air Communications Service, Air Force Communications Service or Air Force Communications Command organization between 1938-1993.

The association has more than 2,600 members. Approximately 85 percent come from enlisted ranks, and 15 percent from the officer ranks, including 35 general officers, both active duty and retired. While we don't maintain specific historical data on our membership, about 35-40 percent are from air traffic control career fields, and 35-40 percent from communications fields. Other members served in a variety of career fields such as command, maintenance, personnel, finance, staff, logistics, administration or flight check.

The association is a non-profit, IRS certified 501 (c) (19) organization with a primary objective of fellowship, and support for Air Force goals and objectives. We're non-political and don't solicit funds for any causes. We support other Air Force-related organizations, such as Air Force Village, Enlisted Widows, Berlin Airlift Historical Association, and Air Force Communications and Information Hall of Fame.

Information on membership and the reunion is available at www.aacsalumni.com (AFCA has a link to our site), or from C.B. "Mac" Maginnis, 6032 S. Bell, Tacoma, WA. 98408, (253) 474-8128, or e-mail Cmagin4375@aol.com.

We encourage active-duty communications and information people who served in any AFCS or AFCC unit to join their predecessors as association members, to share common experiences past and present.

Web site keeps comm and info officers up to date

SCOTT AFB, Ill. — The communications and information officer Web site was designed to provide 33SX officers and civilian equivalents information they may need to support of their careers. It not only provides references to support users in their daily jobs, but also information on professional development, assignments, training and a variety of other topics. One of the unique features that sets this site apart from others is the addition of a discussion bulletin board where users can share "real life" professional and technical information.

"I believe this site has great potential for assisting comm and info officers in meeting their daily challenges," said project manager Maj. Lisa McCoy, Air Force Communications Agency. "33SX officers and civilians can use this site to generate discussions on various issues, ask questions and share lessons learned. We've even included a private discussion group that's restricted to comm group and squadron commanders."

While the site's target audiences are comm and info officers and civilian equivalents, anyone with .mil/.gov access can view the site. However, only registered officers and civilians are granted permission to post messages to the bulletin board. You can visit the site at: https://www.afca.scott.af.mil/33sx/.