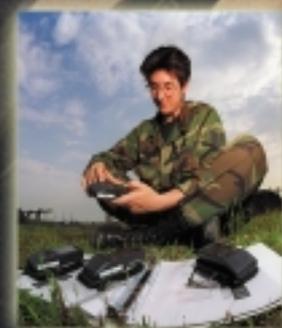


January 2000

# *intercom*

## *Information Assurance In The New Millennium*



# intercom

Volume 41, No. 1

*Commander,*  
*Air Force Communications*  
*and Information Center*  
Lt. Gen. William Donahue

*Commander,*  
*Air Force*  
*Communications Agency*  
Col. Gilbert R. Hawk

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

*Editor*  
Staff Sgt. Michael Leonard

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

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

The 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. Please use high-resolution digital images or 35mm prints.

Mail news copy and photos to AFCA/XPPA, *intercom*, 203 W. Losey St., Room 1060, Scott AFB, IL 62225-5222. The telephone number is DSN 576-4396 or commercial (618) 256-4396. Articles may be sent via e-mail to: [intercom@scott.af.mil](mailto:intercom@scott.af.mil).



✓ Check out our Web site:  
<http://public.afca.scott.af.mil/>

## information assurance

4 U.S. STRATCOM's multiple-layer defense mechanisms yield strong IA posture

8 Information Assurance In The New Millennium events



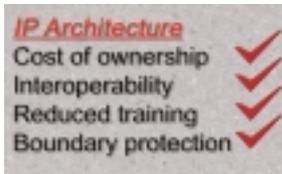
14 Air Force Network Test Center evaluates COTS products for secure comm

18 Information Assurance requires force protection



22 Network security -- everyone's issue

25 Defending a new battlefield -- cyberspace



30 Singing from the 'same sheet of music' with JTA-AF

35 Tools identify weak passwords

37 Assessing the hacker threat

39 AMC's NOSC is state trooper of information highway

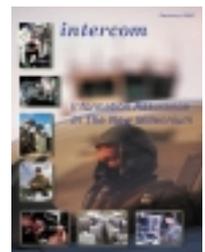
## in other news

41 Ceremony marks opening of GCSS office

43 EIS team enhances Tinker's runway

### About the cover

This month's cover focuses on "Information Assurance in the Next Millennium."



Cover by Staff Sgt. Mike Leonard

# 'Information Assurance In The New Millennium'

By Lt. Gen. William J. Donahue  
Director, Communications and Information,  
Pentagon



Lt. Gen. Donahue

As we move into the new millennium, communications and information professionals should reflect on their accomplishments and be proud of their continuing contribution to the Air Force mission. In contingency after contingency, our nation called on the expertise of the Air Force and you, our Information Warriors, came through with flying colors. You provided the voice, data, and video

services that helped ensure mission success, whether at the "tip of the spear" in combat operations or ensuring network operations in CONUS. The contributions of communications and information professionals provided the reachback, command and control, and information services crucial for our mission success.

Our recent accomplishments are built on the foundation of Information Assurance, providing warfighters information they need — information they can trust — wherever and whenever it's required. We have had a number of successes when it comes to information assurance. We stopped numerous intentional attempts at penetrating our networks and disrupting our operations. We prevented hoards of viruses from damaging our networks and our information. And we successfully survived the major Information Assurance event of our lifetime, the Year 2000 Rollover or Y2K. These are victories in which we can all take pride.

Yet even as we reflect on the successes of the past,

*We must remain vigilant against anything that would interfere with our ability to access and apply information where and when needed.*

it's important to look forward to the challenges the new millennium holds for us. We must constantly strive to improve how we use information in support of air and space operations. We must remain vigilant against anything that would interfere with our ability to access and apply information where and when needed. It is with these thoughts in mind we once again dedicate

*The bedrock of our Information Assurance capability is the cadre of dedicated men and women who support this mission.*

February as Information Assurance Month.

This year's Information Assurance Month theme is "Information Assurance

and it kicks off Feb. 1. We're going to celebrate our victories and pave the way for continued progress in our mission to provide Information Assurance across our Air Force.

The bedrock of our Information Assurance capability is the cadre of dedicated men and women who support this mission. It's no mistake that the "Information Assurance Professional" is the theme for week one of Information Assurance Month. We're going to recognize the "hard-chargers" and the "go-to" men and women making IA work at the unit level. They deserve the "well done." We're also going to focus on professional development of the entire IA team through training and information about the specific situation in your units.

During week two, we're going to expand our scope and work on "Full Dimensional Assurance". Too often we limit our IA thinking to the traditional computer network and the issues of computer network defense. However, information assurance covers a full spectrum of services — voice, data, and video — and involves good operations and maintenance practices, solid configuration management, and all aspects of network management. Is a 99.99 percent network success rate good enough? Ask the 10,000th guy. He might be the one who didn't get the emergency medical treatment because of a network problem — he'll not think it was good enough. We'll use this week to talk about these issues and work on our backup and Continuity of Operations Plans.

We'll return our focus to the individual during week three. The theme is "Good Network Citizenship" and we'll outline the positive characteristics we all need to demonstrate while using the network weapon system. We'll learn what to do to ensure our actions don't adversely affect the network and the critical missions it supports.

"Guardians of the Fifth Dimension" is the theme for week four. The value of networks to the Air Force's mission is not lost on our adversaries. The network is a weapon system and we need to treat it as such. Any complex weapon system has vulnerabilities and the network is no exception. It's definitely a center of grav

See MILLENNIUM Page 5

*intercom*

# U.S. STRATCOM's multiple-layer defense mechanisms yield strong IA posture

By Brig. Gen.  
Trudy H. Clark  
Command, Control,  
Communications  
and Computer  
Systems Director  
U.S. Strategic Command,  
Offutt AFB, Neb.



Brig. Gen. Clark

## Defense-in-Depth Strategy

The U.S. Strategic Command's information security program is a textbook example of a defense-in-depth strategy to insure the availability of its systems and the confidentiality and integrity of its information. STRATCOM uses multiple layers of vendor-independent information defensive mechanisms to achieve a strong Information Assurance posture.

Our first layer of defense is an intrusion detection system, an automated security tool that monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity. STRATCOM is the lead CINC in an on-going program to identify widespread attacks across the DOD, and reports these attacks to the appropriate decision-makers. This is accomplished in three steps.

First, by creating an architecture for the sharing, integration, analysis, and warning of information warfare attacks.

Second, by incorporating legacy and maturing intrusion sensing systems in conjunction with expert systems technology for the management of distributed systems.

Finally, by correlating intrusion events at the local agency, CINC, and

Joint Command levels to tighten the detection grid and increase the success of identifying IW threats. Our intrusion detection system is a key component in identifying and reporting computer network attacks, and keeping our network secure.

External routers provide the next level of STRATCOM's defense. These interconnection devices

are configured to block unwanted IP addresses from entering our networks. Unwanted addresses include sites from which attacks have come or which have a high probability of initiating an attack. These sites are readily available from services or agencies. Once suspect addresses are filtered, it's on to the next layer.

Melissa and BubbleBoy were pointed reminders that e-mail borne viruses and malicious code are still security threats to information systems and networks. To counter those threats at STRATCOM, we installed a mail content scanner. This tool checks the subject and textual content of email against established policy. It also checks for the inclusion of non-textual data, such as video and audio. The mail content scanner is an important tool, and another security level, ensuring our network integrity.

Years ago a vertical metal plate was placed in an automobile for the purpose of keeping an engine fire out of the passenger compartment: it was called a "firewall." In STRATCOM's computer networks, a firewall is a combination of systems that enforces a boundary between "the

evil internet" (the fire) and our internal network (the passenger compartment). The firewall, kept clean of critical data, limits access between external and internal networks in accordance with our security policy. This crucial piece of our network security blocks services, ports, and IP addresses, and logs all important system events such as dropped packets and denied connections. Our firewall configuration provides a formidable network defense.

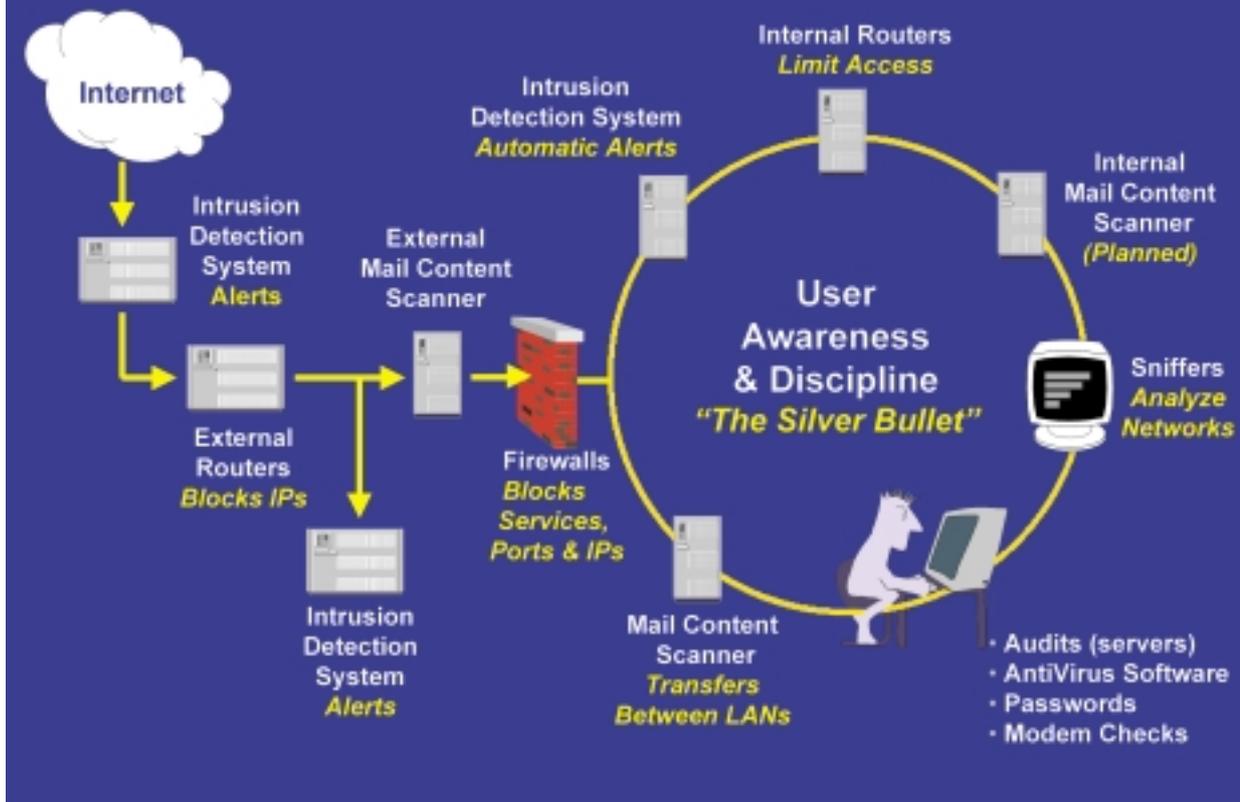
The security tools on STRATCOM's internal network roughly mirror the tools found on the external network – intrusion detection systems, routers, and a mail content scanner which is scheduled for internal implementation during the first part of the year. This mirrored architecture strengthens our IA posture by adding multiple layers of network security mechanisms. The internal routers, for example, strictly limit access to the network for which traffic is destined.

As an added security measure on STRATCOM's internal network, we installed sniffers. Sniffers are powerful network visibility tools used to capture data across a computer network to assist in detailed network

Melissa and BubbleBoy were pointed reminders that e-mail borne viruses and malicious code are still security threats to information systems and networks.

Our intrusion detection system is a key component in identifying and reporting computer network attacks, and keeping our network secure.

# Multi-Layered Defense



analysis. These sniffers are also used by network administrators to diagnose network problems, and determine the proper action to fix them.

STRATCOM uses many other layered security mechanisms. Strong passwords are used for access control and are regularly checked for compliance with our security policy. Host system audits are conducted and reviewed daily for indications of system anomalies. Anti-virus software is frequently updated, centrally managed, and distributed to users.

While all of these mechanisms provide a virtually impenetrable defense against computer network attacks, the most important factor in the equation of IA is user awareness and discipline – the “Silver Bullet” of IA. Through STRATCOM’s quarterly and specialized training, personnel from users to system administrators are given timely, relevant training in a variety of current security topics. As a result, our personnel realize the critical nature of security and take personal responsibility for adhering to sound security policies and procedures.

## Protecting Our Critical Infrastructure

STRATCOM’s information security professionals are actively working to fulfill Presidential Decision Directive 63. The directive calls for a closely coordinated

public-private information-sharing partnership with government to eliminate the potential vulnerabilities to the entities which make up our critical information infrastructure – Information and Communications, Electrical Power Systems, Gas and Oil Transportation and Storage, Banking and Finance, Transportation, Water Supply Systems, Emergency Services, and Government Services. Several initiatives are underway which are producing encouraging results in the community.

In May 1999, STRATCOM hosted the Omaha Cyber Security Conference. This event targeted CIOs and security managers in critical infrastructure companies in the Omaha, Neb., area. More than 100 representatives from Fortune 500 companies, state and municipal government, and others gathered at Offutt AFB to share in this first of a kind conference.

At the Omaha Cyber Security Conference, two corporations, Science Applications International Corporation and the Applied Information Management Institute, volunteered to continue the efforts to increase awareness in Omaha. A monthly meeting, the Cyber Security Forum, was established to share information

# Information assurance is not just protecting and defending the mission

By Brig. Gen. Dale W. Meyerrose

*Air Combat Command Director of Communications  
Langley Air Force Base, Va.*

The Air Force's Global Engagement mission and posture as an Expeditionary Air Force are information intensive endeavors. With the explosive growth of information technology, a corresponding information dependency has developed as an integral part of combat operations. Consequently, mission accomplishment is increasingly dependent upon Information Assurance.

Information Assurance ... now there's a phrase with a lot of baggage and too many meanings. Our current Information Assurance programs grew out of earlier computer security and information protection programs. Unfortunately, too many of us still look at Information Assurance as a "protect and defend" mission. By focusing on protection, much of our information assurance

workload becomes reactive. This level of uncertainty puts us all behind the power curve. While protection is important, it's important for us to understand the total scope of Information Assurance.

To us, *Information Assurance is providing reliable, operationally ready networks that provide the right information, at the right time, to the right place, in the right format.*

From this definition, it is clear that providing full-spectrum Information Assurance requires a critical change in how we operate, protect, and upgrade the enterprise and how we train all network operators and users. The following addresses these key components:

**Operate:** First, let's agree that communications and information professionals *operate* the network weapons system. We provide 24 x 7 command and control of all network functions and equipment through the AFNOC, MAJCOM NOSCs, and base NCCs. We perform network management, optimization, fault detection and resolution, and a variety of other tasks.

We are responsible for the health of the network. As network operators, we are primarily concerned with moving information. Through OPREP-3 reports, SORTS, and INFOCONs, we give senior leaders, users, and our communicators a deeper understanding of the operational status of the network. Performing this

awesome responsibility requires us to approach the task in a disciplined and standardized way. ACC recently completed a Tactics, Techniques, and Procedures manual for the network weapons system.

The TTP manual outlines standard equipment and personnel formations, rules of engagement for various network events, and adds structure to our network C2 and enterprise management actions. I hope you all have a chance to review our manual and join with us to make it a better, more useful document.

**Protect:** Protecting information and information systems is the second pillar of our Information Assurance construct. We adopted a "defense in depth" approach to protection. We're working very hard to move all systems and circuits behind the protection of Base Information Protection tools installed in our NCCs and monitored by intrusion detection systems such as ASIM.

We developed and delivered, to all ACC bases, an automatic virus definition file checker and dissemination system. Upon login, the system checks the installed virus definition file against the most current and downloads and installs an update as needed. We've basically taken the user out of the loop.

In a similar initiative, we're installing Microsoft's Systems Management Server on every ACC computer on an ACC base. Once installed, we will automate the dissemination of all AFCERT patches. SMS will also automatically verify that the patch was successfully installed. We are also partnering with the Air Force Research Lab to develop and test a system that collects, analyzes, correlates, and displays security events from across the ACC enterprise. Our goal is to field a single console in our NOSC that provides a complete picture of the security posture of our network.

**Upgrade:** This pillar speaks to our need to modify the way we modify our enterprise. We can no longer install software or equipment on the enterprise without a thorough analysis. I can safely say that well-meaning folks inappropriately changing the enterprise caused the vast majority of enterprise downtime -- we call this a self-inflicted denial-of-service attack. We continue to be held hostage by every program manager on



**Brig. Gen. Meyerrose**

... it is clear that providing full-spectrum Information Assurance requires a critical change in how we operate, protect, and upgrade the enterprise and how we train all network operators and users.

See **MISSION** Page 7

## MISSION

From Page 4

an individual basis . . . and we continue to learn the same mistake with every program at every base.

To combat this growing trend, we made the NOSC responsible for controlling all changes to the ACC enterprise. The NOSC executes our change management process. A key component of this process is our Certificate to Operate. The CTO is a joint effort between ACC/SC and the functional representative wishing to place a mission application on the Enterprise.

The CTO addresses the application's capabilities, limitations, potential risk, logistics support, and training. The certifying process is ACC's method for establishing accountability and maintaining configuration control of mission applications and the enterprise. In addition, the NOSC will oversee operational testing to ensure new systems and applications are working properly and not adversely affecting any other aspect of our enterprise operations.

**Train:** It's clear to us that being able to provide reliable and operationally ready networks requires a professional, dedicated, and skilled workforce. The Air Force took a giant step when it published AFI 33-115 Vol 2. Providing a standardized and structured training program is certainly the foundation of any successful operation. However, in ACC, we will make the distinction between training and certification. Training is simply the acquiring or improving of skills. Trainers and instructors provide training. Certification on the other hand is authorization to employ knowledge and skills to meet mission needs.

Only commanders can certify mission qualifications. Our training efforts extend well beyond the communications squadron to every network user in ACC. Through annual Security Awareness Training and Education we will make sure everyone knows their Information Assurance responsibility.

*Providing a standardized and structured training program is certainly the foundation of any successful operation.*

We've added an Information Assurance Cliffnotes link of the ACC/SC webpage to help wing commanders focus their efforts. And finally, we're getting tremendous support and direction from the Commander of ACC, Gen. Ed Eberhart. He sent a memo to all wing and NAF commanders telling them, "Each of you is the senior Information Assurance officer in your wing -- much like you are the senior flight safety officer and force protection officer." Talk about raising Information Assurance awareness!

Let me share some thoughts on Information Assurance Month. Information Assurance, like many other important Air Force programs is a continuous journey. While it's great to increase awareness during one month each year, we need to make it more visible all year. How often do commanders stress safety? Constantly. How about Information Assurance? Probably not enough. In ACC, we've developed an Information Assurance 2000 strategy that leverages the Air Force's Information Assurance Month program into a year-long program.

In February, we'll kick off our year-long program. The ACC/SC staff is preparing Information Assurance articles, briefings, and posters to send to our bases. We hope to do much of the time-consuming work here and ship the products to ACC bases to execute.

Once February has come and gone, our program will still be turning. At least once each quarter, we'll author an article for base newspapers and build a briefing the communications squadrons can take to other units' Commander's Calls. We will make significant gains only if we make Information Assurance persuasive in our thinking, attitudes, and culture.

Information Assurance is our contribution to Expeditionary Aerospace Force operations. Our warfighters need each and every one of you completely engaged and working hard to provide the most reliable, operationally available, capable, and protected enterprise possible. Please join me in searching for innovative solutions to these tough challenges.

## MILLENNIUM

From Page 3

ity for our adversaries with malicious intent. There are also those who seek the recognition of their peers by breaking into our systems or instigating computer viruses. Each can be damaging to our mission and we must guard against them with the same rigor and tenacity as exhibited by Security Forces personnel at our front gates. This week we'll focus on the pieces which provide that protection, both human

and technical.

Finally, we'll wrap everything up in week five with a celebration of the last Y2K hurdle — the leap year rollover. We've been proactively working the Y2K problem for a long time. We'll "stay at our posts" until the sun rises March 1 and celebrate "Y2K Victory Day". Y2K is an information assurance issue of the first order, and the enduring lesson from Y2K will be the fact our Air Force, and society at large, depends on information, and information technology for all of our essential

mission and business processes — information assurance must be the communication and information professional's hallmark of excellence — trusted information, any time, any place.

February will be a busy month. I hope each and every one of you takes this opportunity to expand your knowledge and commitment to the principles of Information Assurance. Together, we can do our part to ensure the continued success of our Air Force and our great nation into the new millennium.

# "INFORMATION ASSURANCE IN THE NEW MILLENNIUM"

## Week 1 - Professionals

Focus on education and emphasize completion of IA Internet Based Training and professional development. Recognize IA professionals.

Suggested Activities:

- \* Complete required IA IBT courses throughout the year, not just in February.
- \* Schedule, contact, or complete IA professional development classes or seminars.
- \* Recognize and reward outstanding IA professionals.
- \* Conduct a combined base Network Steering Group or COMPUSEC manager meeting focusing on IA issues.

## Week 2 - Full Dimensional Assurance

Full dimensional assurance involves more than just computers and data; it also includes voice and video communications media. Consider configuration management, following proper procedures, operational management of networks, preventive and routine maintenance, ensuring back-up power is available and users know how to operate it, ensuring users back up software, ensuring contingency plans include alternate processing locations and are practiced, establishing restoral priorities, planning for redundant routing. Emphasize resilient, dependable networks.

Suggested Activities:

- \* Implement Base Information Protection tool configuration templates to standardize configuration of BIP tool suites across the Air Force.
- \* Review and update restoral priorities for voice, video, and data networks and coordinate any changes with customers.
- \* Exercise contingency back-up plans.

## Week 3 - Network Citizenship

Focus on abuse as opposed to people hacking into our networks. Emphasize discipline, e-mail etiquette, software piracy, inappropriate behavior (cell phone, DSN, etc.) Quality of service depends on discipline.

Suggested Activities:

- \* Reinforce rules for network use. Abuse of information systems is as much of a problem as hackers.
- \* Emphasize that government systems are for official use only.
- \* Update policy letter establishing guidelines on the use of information systems for official business..
- \* Educate users about software piracy.
- \* Complete software piracy CBT.
- \* Promote self-discipline to increase quality of service.
- \* Limit length of telephone conversations.
- \* Adhere to established limits for the sizes of files transmitted over e-mail.
- \* Complete cyberspace clean-up of web pages, shared drives, and personal drives, etc.
- \* Issue JA position on responsibilities and rights when monitoring computer/network activity.

## Week 4 - Guardians of the Fifth Dimension

Focus on protection pieces of IA. Kick off the 2000 Telecommunications Monitoring and Assessment Program certification process. Emphasize protection procedures. Stress IA and operational availability.

Suggested activities.

- \* Emphasize network protection mechanisms.
- \* Kick off TMAP certification process.
- \* Explain the use of firewalls and proxy servers.
- \* Provide encryption/protection policy, guidance, and options.
- \* Ensure current anti-virus software is installed and signature files are updated.
- \* Confirm local release procedures are in effect for checking different types of information on local web sites.
- \* Revitalize OPSEC working group to update critical information lists.
- \* Rekey STU-IIIs.

## Week 5 - Y2K Victory

Focus on Feb. 29 as the last hurdle of the Y2K effort—the largest single information assurance challenge in history.

Wrap up the millennium challenge with a joint celebration.

Suggested activities.

- \* Release information Feb. 24 stressing the need for vigilance on Feb 29 as the last Y2K hurdle. Celebrate Y2K victory.
- \* Release success stories from Jan.1 rollover.

# STRATCOM's multiple-layer defense mechanisms yield strong IA posture

From Page 5

between interested individuals and companies. More than 30 participants regularly attend these meetings where information security topics are discussed.

The National Information Protection Center is the national focal point for threat assessment, warning, investigation, and response to attacks on the critical infrastructure. The NIPC is working with representatives from the infrastructure areas to form local Infragard Chapters, vehicles through which to share threats, intrusion incidents, system vulnerabilities, and interdependencies of the infrastructure. An integral part of the NIPC is the local FBI Field Office, a catalyst in the process of engendering cooperation and support for the implementation of PDD 63.

As a result of local FBI agents' presentations at the Omaha Cyber Security Conference and at the Cyber Security Forums, an Omaha Infragard Chapter was formed with several corporations coming on board and more to follow.

Infragard will have two components: an Alert Network to allow members to communicate via secure e-mail, and a website where computer security information and links to other security sites will be posted. The membership of Infragard is anonymous by design to facilitate the sharing of sensitive information without attribution. Establishing the Omaha Infragard Chapter brings the NIPC a step closer to their goal of having a nation-wide organization of public-private corporations sharing intrusions, known vulnerabilities, and corrective actions to protect our national information infrastructure.

Another initiative which will ultimately strengthen our national security posture is STRATCOM's partnership with the Peter Kiewit Institute of Information Science, Technology and Engineering. The Institute, housed in a \$70 million, 192,000-square-foot state-of-the-art building, is a merger of the University of Ne-

braska at Omaha's College of Information Science & Technology and the University of Nebraska-Lincoln's College of Engineering & Technology. The collaborative partnership was formed to meet the increasing need for information technology professionals in the Omaha area and around the nation.

The Peter Kiewit Institute asked STRATCOM to participate in a forum with academicians and local business leaders to recommend changes to the Institute's under-graduate and graduate curriculum. The recommendation to include a "Cyber Security Track" composed of five to six courses for a specialized certification program in information security was overwhelmingly endorsed by area business representatives.

STRATCOM believes this track will satisfy a vital need to increase knowledge in the area of Information Assurance.

Realizing the importance of first-hand cybersecurity experience, more than 20 of STRATCOM's information technology professionals volunteered their time to personally mentor Peter Kiewit Institute students. This partnering of students and mentors exposes the students to invaluable, practical computer security principles, and provides job opportunities for the students. STRATCOM will hire six

students as interns starting in January, using the Office of Personnel Management's Student Temporary Employment Program. Six students were hired last summer by contractors working with STRATCOM.

STRATCOM's mission is Strategic Deterrence. Our bottom line is that a strong cyber-security program is essential to protect our critical command and control information systems. Our zeal for strong security and our willingness to share our expertise is helping to protect the national information infrastructure, and is guiding and mentoring some of the brightest information technology students in the nation. STRATCOM's efforts and initiatives will continue to yield local and national dividends well into the next millennium.



# Aunt Judy and the 'Virus of Doom'

By Staff Sgt. Jeremy Riley

Network Control Center, McConnell AFB, Kan.

Nov. 11 started out like any other day. I rolled into work, vowing for the fourth time that week to go to bed early tonight. I poured myself a half-gallon of 98 octane Java, and sat down to check my e-mail.

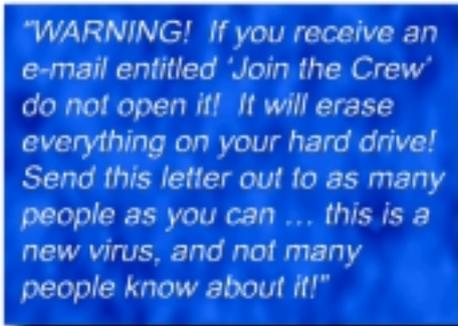
Awaiting me in my mailbox was an e-mail with an ominous subject line – "VIRUS WARNING!". Working in the Wing Information Assurance Office, this naturally piqued my interest. Had the Air Force discovered a new virus that computer users at McConnell needed to be informed about? Were we possibly infected already? Would I have to re-arrange my time-management schedule?

With a trigger-finger that would make Wyatt Earp proud, I fired off two clicks on my mouse and up popped the message. The first thing I noticed was that it wasn't from someone in the Info Assurance world, or any other DOD activity for that matter.

This one was from Aunt Judy, who is as sweet a lady as you'd ever care to meet, but hardly an authority on computer viruses. Nonetheless, I read on. After all, she'd sent me a box of cookies last week.

It was a message she had received and forwarded to me. It read:

*"WARNING! If you receive an e-mail entitled 'Join the Crew' do not open it! It will erase everything on your hard drive! Send this letter out to as many people as you can...this is a new virus, and not many people know about it!"*



Undoubtedly, Aunt Judy was extremely concerned for the welfare of her friends and family when she learned of this catastrophic new virus. With a heart as big as Texas, and hair to match, she'd followed the message's instructions and sent it to everyone she knew. Forty-seven people, to be exact.

What Aunt Judy didn't know is that no such virus exists. The e-mail she forwarded was an electronic hoax and potentially damaging to our security.

You're probably asking yourself why someone would take the time to create and send a hoax message. I bet you're also wondering why it would pose a danger to our security.

An e-mail hoax is designed with a singular purpose – to overload networks. The creators of these hoaxes exploit the trusting nature of people like Aunt Judy and many other computer users. They appeal to our desire to protect our friends or inform others of important information. They expect the users to forward the message, just as the creator instructs, to friends, family,

and co-workers. In turn, they expect those recipients to do the same, and so on. Before long, the message has been replicated so many times that networks become bogged down, processing slows, and high-powered servers can even crash. In the computer security world we refer to this as a denial of service and its impact can be immeasurable.

Remember, Aunt Judy forwarded the hoax to 47 people. Let's say they do the same thing. Suddenly, 2,209 copies of that single e-mail exist after just two cycles. After three cycles, 103,823 copies are floating around. After 10 cycles, here's the number: 5.259913223583e+16. I checked with Aunt Judy and she didn't know what that equaled, but we both agreed that it was pretty big.

If that isn't bad enough, consider that this hoax has been passed around over and over for several years. It's received by random users at McConnell every week. And "Join the Crew" is just one example of hundreds, possibly thousands, of hoaxes that are circulating via the Internet. There are many others, ranging from the

traditional "Forward for good luck" message, to hoaxes that claim a certain charity will make a donation to a sick child each time you forward it.

So, as a user, how do you and Aunt Judy sift through what's real and what's a fraud?

First, anytime you receive a virus warning via e-mail you should immediately be suspicious – do not forward it! Call your Unit

COMPUSEC Manager or the Wing IA office to verify its legitimacy. If the warning is valid, the IA office will take steps to warn the base populace.

Second, know how to recognize a hoax. Any e-mail that requests you forward it should be viewed with suspicion. Don't be fooled if the e-mail seems to come from a reputable source, such as a big name computer company or a major university – it's all a part of the hoax! Bill Gates isn't going to give you \$1,000 for forwarding his message, as promised in a ridiculous hoax recently.

We all try to take care of each other and the originators of these hoaxes attempt to take advantage of that.

Fortunately, the Air Force has established the Information Assurance office to make sure you are taken care of and that the proper procedures are followed.

By understanding the nature and purpose of these hoaxes, you can help stop an adversary from causing a denial of service and impacting our mission.

It might just keep Aunt Judy's mailbox a little cleaner.

# You are subject to being monitored

By Wayne Phillips and  
Charles Laedlein  
Air Force Communications  
Agency, Scott AFB, Ill.

You've seen it numerous times. In fact, it has become so routine that you probably are unaware as to why it's there and what it really means. You see it every morning when you first power up your computer and you see it every time you pick up your telephone on your desk. What is it? Acknowledging that you are subject to being monitored whenever you use any telecommunications device. Remember the notice and consent banner that appears when you first turn on your computer in the morning (the screen that keeps staring at you until you hit a key to go on)? How about that sticker (DD Form 2056) that keeps trying to peel off your phone?

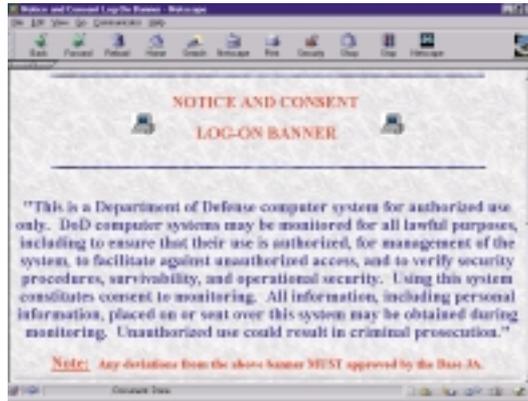
Biennially, during even-numbered fiscal years each base/site must be certified for telecommunication monitoring by the Secretary of the Air Force General Counsel. This is accomplished by completing the requirements in AFI 33-219, *Telecommunications Monitoring and Assessment Program*.

Each base must certify that they have legally notified all personnel that use of telecommunications devices constitutes consent to TMAP monitoring. The most common telecommunications devices are telephones, computers, fax machines, cellular telephones, and hand-held radios. As technology evolves, so will the list.

Authority to continue base monitoring rests with the Air Force General Counsel. Following the last TMAP review, the Air Force was informed not to expect any temporary extensions. It will come down to either you are 100 percent compliant or not.

TMAP is a key part of the Air Force's Operations Security efforts. AFI 33-219 permits monitoring of unsecured telecommunications systems to determine vulnerability to hostile signal intelligence exploitation. However, because TMAP involves surveillance of base communication systems, the Air Force Instruction contains very clear, concise, mandatory notification procedures that must be in place to support this program. To ensure compliance, the instruction requires an extensive review of base or organizational user notification processes every two years.

A critical part of the TMAP certification process is the requirement for legal review at base and MAJCOM levels. In addition, the AFI requires further review by the Air Force Communications Agency and the Air Force General Counsel. It is important base communi-



cators work closely with their legal counterparts in conducting TMAP surveys and preparing reports.

Despite what appears to be very clear guidance, a number of bases encountered serious problems accomplishing the last TMAP review and reporting. While those of us in the review process have enjoyed the brickbats and colorful suggestions resulting from the return of base

TMAP packages, we are working to make the process less painful for all concerned in the future.

Although your base legal folks are responsible for the initial reviews and ensuring compliance with AFI 33-219 requirements, it is imperative you too understand the rules of the game.

The purpose of legal reviews is to certify that users of telecommunications devices have been provided sufficient notice of consent to monitoring. In other words, the documentation included in report packages should clearly confirm that base notification efforts meet the instruction's specific requirements, and that users of base telecommunications are placed on notice that their calls, e-mails, or faxes are subject to monitoring.

Rules of engagement concerning TMAP are in Attachment 2 to AFI 33-219. Key requirements include:

- \* A consent statement prominently *displayed on the front cover* of base/organizational telephone directories
- \* A DD Form 2056, Telephone Monitoring Notification Decal, placed on all telephones subject to monitoring
- \* A DD Form 2056 sticker on all fax machines and the mandatory use of AF Form 3535, Facsimile Electro Mail transmittal, to be used as a fax cover document IAW DODD 4525.8/AF Sup 1, Official Mail Manual
- \* Either a DD Form 2056 decal affixed to all cellular phones and hand-held radios, or a consent form letter signed and dated by the user
- \* A notice of monitoring log-on banner installed on all computers.

These requirements are quite specific, and base certification packages should contain sufficient information to confirm all communications users are put on notice that use of base telecommunications equipment constitutes consent to monitoring. If you have other communication equipment subject to monitoring, such as text pagers, be sure to provide some notification of monitoring using the processes above.

Problems arise in the review process when requirements are not clearly addressed. For example, if a pack

See TMAP Page 12

# AF computer network pros battle viruses

WASHINGTON, D.C. — While many people were working on their plans to welcome the new millennium, Air Force computer network professionals have been working on war plans. The battle is against computer viruses. It was feared that terrorists, hostile nations, criminals, and “thrill-seeker” hackers could all launch attacks on government and private sector computers at the same time—and could use Y2K malfunctions to hide their actions.

New, fast-spreading and potentially dangerous strains and variants have been appearing. There has been some fear that many new, even more destructive viruses may appear as hackers try to create a doomsday scenario related to Y2K.

An increase in e-mails and electronic greeting cards that people are sending during the holidays offer virus writers a good means to pass along their bugs, according to computer security experts.

Some Y2K-related viruses that have surfaced include W32.Mypics.Worm, or Mypics. Mypics arrives as an e-mail attachment posing as pictures from a friend that, if opened, will replicate and send itself to as many as 50 people from the victim’s address book.

If undetected, the virus will hide on the infected user’s computer. It will wait until a certain date when the computer is turned on and then delete files on the victim’s hard drive and prevent rebooting, according to computer security experts.

The past year has been marked by a wave of destructive infections, including the CIH, or Chernobyl Virus, which wiped out data on thousands of hard disk drives, and Melissa, which was one of the most widespread infections ever, though not as damaging to indi-

vidual computers. Melissa struck on March 26, disguised as an “important message” from a friend or colleague, and spread around the world like an electronic chain letter.

“The threat is rapidly evolving; our networks are undergoing explosive growth, and a single vulnerability in the network exposes everyone to the real risk of mission compromise,” said Lt. Gen. William Donahue, Air Force director of communications and information. “We must continue to improve our capabilities in the network arena. We need to beef up our training for network professionals and users, and we need to treat our networks like the critical weapon systems they have become,” he said.

All users of Air Force computers should be aware of the dangers and educate themselves about mass-mailing viruses called worms, and date-triggered viruses. Even though the threat is real, users should be aware that there is also a lot of hype. The key to avoiding viruses is awareness. Most important is having reliable antivirus software.

Home users can protect themselves by taking advantage of enterprise level anti-virus software programs that extend to AF personnel and their home computers and/or free antivirus software for personal use downloadable from the internet. Computer security experts sounded an alarm to limit the spread of the viruses. The most basic advice they give is to avoid opening unsolicited and suspicious e-mails on computers.

“We must remain vigilant against anything that would interfere with our ability to access and apply information where and when needed,” said General Donahue.

---

## TMAP

*From page 11*

age indicates a random survey of telephones established 95 percent of phones had a DD Form 2056 decal, your legal counterpart is sure to question the scope of the “survey” -- whether it included all phones on base or consisted of a smaller sample like all telephones in the base commander’s office (there is a difference in scale). The report should also describe what action was taken to correct the five percent of phones lacking required stickers.

Remember that the TMAP certification process is not intended to be a pencil-whipping exercise. If the evidence is not sufficient to establish compliance with the AFI, rest assured a report will be returned for

more documentation. Such returns cause serious delays in certifying compliance and may result in suspension of monitoring authorization.

There are numerous additional, optional methods to inform users of communications monitoring. One of the things you could do is to publish articles in the base newspaper, the base bulletin, on the base Intranet, in newcomers orientations or as part of commander’s calls. Don’t forget those geographically separated units supported by your base. Ask yourself, who supports their telephones and networks? If it’s your base, they need to be included in your TMAP report. When in doubt, ask your base legal office for assistance.

You may ask, why cover all this now? Experience has demonstrated several months is not too long a pe-

riod for meaningful, effective surveys of all base telecommunications equipment and correction of deficiencies in providing monitoring notices to users. It also is not too soon to initiate good documentation of TMAP inspections. Although your base certification may be for a two-year period, you should conduct continuing checks for notice decals and banners on your comm equipment. A little effort now will make life easier for all TMAP certification participants.

Contact your base legal office for more assistance or information and they in turn can call AFCA/JA if necessary. We would prefer to help you now instead of criticizing your efforts tomorrow. The TMAP point of contact is Wayne Phillips, AFCA, DSN 576-2121.

# 'Networthy' systems ensure Info Assurance

By Patricia Mineer

Air Force Communications Agency, Scott AFB, Ill.

For years, the problems encountered when fielding weapon systems and automated information systems have highlighted the need to increase the visibility of C4I support requirements early in the acquisition/development process. Problems have ranged from the installation site having incompatible network systems that couldn't operate with the new system to saturated networks incapable of accepting more computer traffic.

Other issues such as weak security or high risks associated with the new system's operations or protocols have been identified and have slowed or stopped system installations. These, and similar problems have one thing in common -- all are expensive to fix!

The C4ISP is the tool for providing needed visibility into program/system development. The mature C4ISP includes operational, system, and technical architecture views; security policy, System Security Authorization Agreement; schedule and cost information; workload, testing and training considerations; and derived C4I support requirements, shortfalls, and possible solutions.

The communications and information community uses the C4ISP to evaluate "networthiness" of systems. The term "networthy" is used to describe the suitability of a system (hardware or software) to be implemented, operated, and maintained in a specified environment. A system deemed to be networthy can be implemented and sustained while providing its intended functionality in a specified environment without degrading the environment beyond specified limits or introducing unacceptable security risks.

Parameters to be evaluated include, but are not limited to, network utilization, latency, protocols, network size/topology, security, compatibility with existing hardware/software, interoperability, compliance with standards, logistics support, user training requirements, and certification of spectrum use.

Assessment is performed by the comm and info community throughout system development so that any issues can be addressed early, when fixes are more economically feasible. Generally, assessment begins with desktop analysis of C4ISP documentation. The analysis identifies systems that will fail functionally, cause major problems on operational networks, or introduce security hazards.

After desktop analysis, the system proceeds to testing. Testing is done to establish the level of confidence required for Air Force approval. This testing will typically be done at a government testing facility like the Air Force Network Test Center at Air Force Communications Agency.

A *Certificate of Networthiness* is issued to sys-

tems that pose no unacceptable level of risk or operational impact to operational networks.

- \* System will work as expected on operational networks—no undue burden

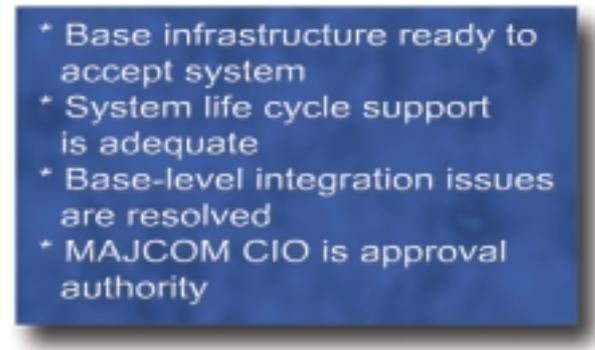
- \* System does not introduce unacceptable security risks

- \* System is supportable

- \* Comm & Info shortfalls have been identified and managed

Air Force or major command CIO is the approval authority for the *Certificate of Networthiness*, depending on system type/level.

The affected MAJCOMs will be kept in the loop throughout system development and will not be taken by surprise by the imminent arrival of the system. Issuance of the *Certificate of Networthiness* is the trigger for further evaluation by MAJCOMs to ensure systems will operate at specific Air Force bases. The *Certificate to Operate* is issued by MAJCOM/CIOs to systems that pose no unacceptable level of risk or operational impact to the MAJCOM and Base Enterprise.



This evaluation process primarily involves desktop analysis to identify any late problems associated with the AF bases designated for system installation.

The C4ISP/*Certificate of Networthiness* produces fantastic results benefiting all parties—PMOs, MAJCOMs, bases, users, providers, and the Air Force. It incorporates a disciplined process for identifying comm and info support requirements. It plugs the comm and info community into the security certification and accreditation process where we can do the most good — early. It provides an avenue for attacking disconnects between actual needs and in-place infrastructure. It ultimately ensures comm and info support to the right people at the right time ... successful fielding of functional mission systems ... Information Assurance.

For more information on C4ISP development, refer to DOD 5000.2R and the DOD Acquisition Deskbook. The C4ISP is one of only two mandatory decision documents for all systems/programs. Air Force efforts, in lockstep with OSD, are on-going and include policy and procedure development. Please call AFCA/ITLD, DSN 576-3489, for updates on OSD or AF C4ISP efforts.

# AF Network Test Center evaluates COTS products for secure comm

By Walter Patton

*Air Force Communications Agency*



*Photos by Jack Root*

**Master Sgt. Greg Heck installs a cable that connects a deployed test infrastructure with Scott AFB's fixed-base environment.**

**SCOTT AIR FORCE BASE, Ill.** — Information assurance testing to verify network security is one major test conducted for all data systems in the Air Force Network Test Center. In the past six months, engineers in the center have evaluated commercial-off-the-shelf products that provide secure communications.

The products evaluated included next-generation secure terminal equipment; a commercial low-cost, small-sized encryption device; a software application that allows users to work together between remote locations; and COTS hardware encryption cards that provide information assurance to virtual private networks.

The Center, located at Scott AFB, is designed with the capability to connect to other DOD test facilities to share resources for collaborative testing of information technology systems. It provides a unique capability to assess and manage risks associated with fielding new network components, systems, and software.

Established in the Air Force Communications Agency's Technology Interoperability Facility, the Network Test Center can emulate a wide range of network configurations and scenarios.

Operation of the Center requires a combination of hardware, software and people with the correct skills and experience. Center support ranges from developing detailed test plans, conducting tests, and preparing reports, to coordinating facility use by technically knowledgeable customers.

The Center was recently used to develop the firewall configuration for the Air Mobility Command's Command and Control Information Processing System.

Military and civilian engineers from AFCA's Glo-

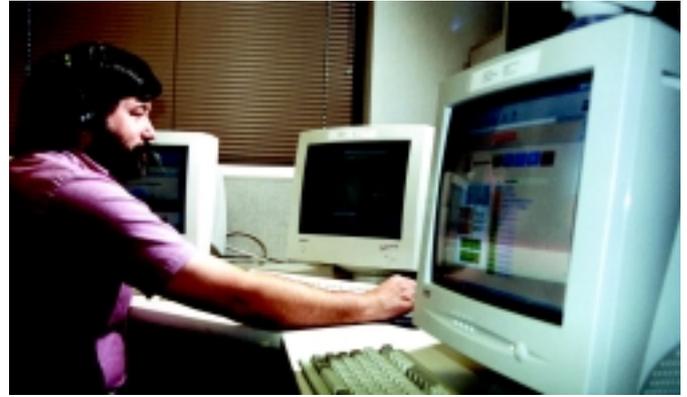
bal Connectivity Directorate used the Center's facility to test firewall and other Base Information Protect equipment solutions before fielding them and to evaluate potential IP tools. GC engineers and engineers from AFCA's Technology Directorate cooperated in seeking firewall switching agents and virtual private network solutions.

**Jane Guidicini, AFCA, evaluates secure terminal equipment (black telephone unit) that assures secure video-conferencing between desktop computers.**





**Capt. Francis Afinidad installs an Internet protocol secure hardware encryption card into a computer to provide a secure virtual private network.**



**Tom Benignus runs performance tests in a COTS software program that allows users in remote locations to communicate securely.**

Other major types of testing conducted in the Center for all data systems include:

- \* System integration encompassing all test requirements for a typical base installation.

- \* End-to-end tests that measure proper functionality from a host to a client.

- \* The main hardware and software elements of the Center are base infrastructure emulation (in-garrison and deployed), inter-base connectivity emulation, functional applications, and monitoring and measurement tools.

The Center's base infrastructure design includes hardware that provides the capability to simulate network traffic and measure key network parameters. The Center can simultaneously emulate at least two scalable main operating base networks and five geographically separated units. The emulation environment accommodates testing for combinations of small, medium, and large bases.

Three major Combat Information Transport System components are used in the Center to imitate base infrastructures: Information Transport System, the Network Management System/Base Information Protect System, and the Voice Switching System.

Emulated non-secure and secure wide area networks (NIPRNET/SIPRNET) connect the Center's in-garrison and deployed elements. Emulation of the NIPRNET and SIPRNET is based upon engineering approximations of real-world configurations including multiple routers, bulk encryption, and serial communications links.

The Center's test team develops reports documenting the objectives, test processes, and test results and the success or failure of each test objective.

To schedule use of the facility call DSN 576-3700/3720 or send a fax to (618) 256-8952.



**Tim Maas evaluates a small, low-cost encryption device that replaces much larger encryption devices previously used to provide secure videoconferencing capability.**

# Network Management System/Base Information Protection modernizes bases using a phased approach

By Lt. Col. Howard L. Borst  
*Electronic Security Command*

The Combat Information Transport System is a commercial-off-the-shelf-based, Air Force-wide program designed to modernize the information transport capability at the base level. CITS replaces maintenance intensive equipment, replaces or upgrades existing voice switching systems, provides network management of information systems, increases the capacity of saturated information transmission systems, and provides information protection tools. There are four distinct product areas of CITS designed to meet these requirements:

- Information Transport System
- Network Management System/Base Information Protection
- Voice Switching System
- Telecommunications Management System

While each of these product areas is an integral component of the CITS program, this article focuses on the capabilities of NMS/BIP.

The Network Management System provides centralized command and control information assurance tools to the network control centers, and consolidates/standardizes network management operations and information assurance for the base. The base information protection portion of the CITS program provides layered defense information protection tools to detect, deter, isolate, contain, reconstitute, and recover from information systems and network security intrusions or attacks.

To avoid overwhelming the bases with an excessive amount of tools at one time (a lesson learned from the baseline prototype installation), the NMS/BIP program was restructured use a phased approach, training the NCC personnel at the end of each phase.

Phase 1, implemented in 1998, provided a firewall between an external router connected to the Air Force Internet and an internal router connected to the base network. A shunt was put in place as a temporary measure to permit continued operation of subnets of the base network that relied on certain functionality that would be disallowed by the firewall. The shunt is simply a network connection between the external switch and the internal switch bypassing the firewall. During the implementation of Phase 1, five subnets were placed

entirely behind the firewall. The NCC staff was trained to migrate the remainder of the base on a schedule that permitted the base tenants to retire, replace, or modify legacy capabilities to conform to the security policy enforced by the firewall and base routers.

Phase 1 also provided a proxy server to facilitate access to external network services including http (the web), telnet (terminal access), and ftp (file transfer); a network management system to manage the base network; a GPS time server to synchronize host clocks; and a backup system to ensure recovery of critical base systems in the event of a system failure. Three management workstations were provided to facilitate system operations and maintenance. Finally, auxiliary battery power was provided for continuity of operations during periods of power outages.

Phase 2 implementations began in July 1999, and will continue through spring 2001. This phase adds four capabilities to those already provided in Phase 1.

First, it provides a standardized Domain Name Service, which consists of an external primary DNS server to resolve internet queries about publicly accessible base hosts/services (e.g., e-mail message transfer agents and web servers), an internal primary DNS server for resolving queries originating inside the base, and an IP management capability to simplify management of the base IP address space.

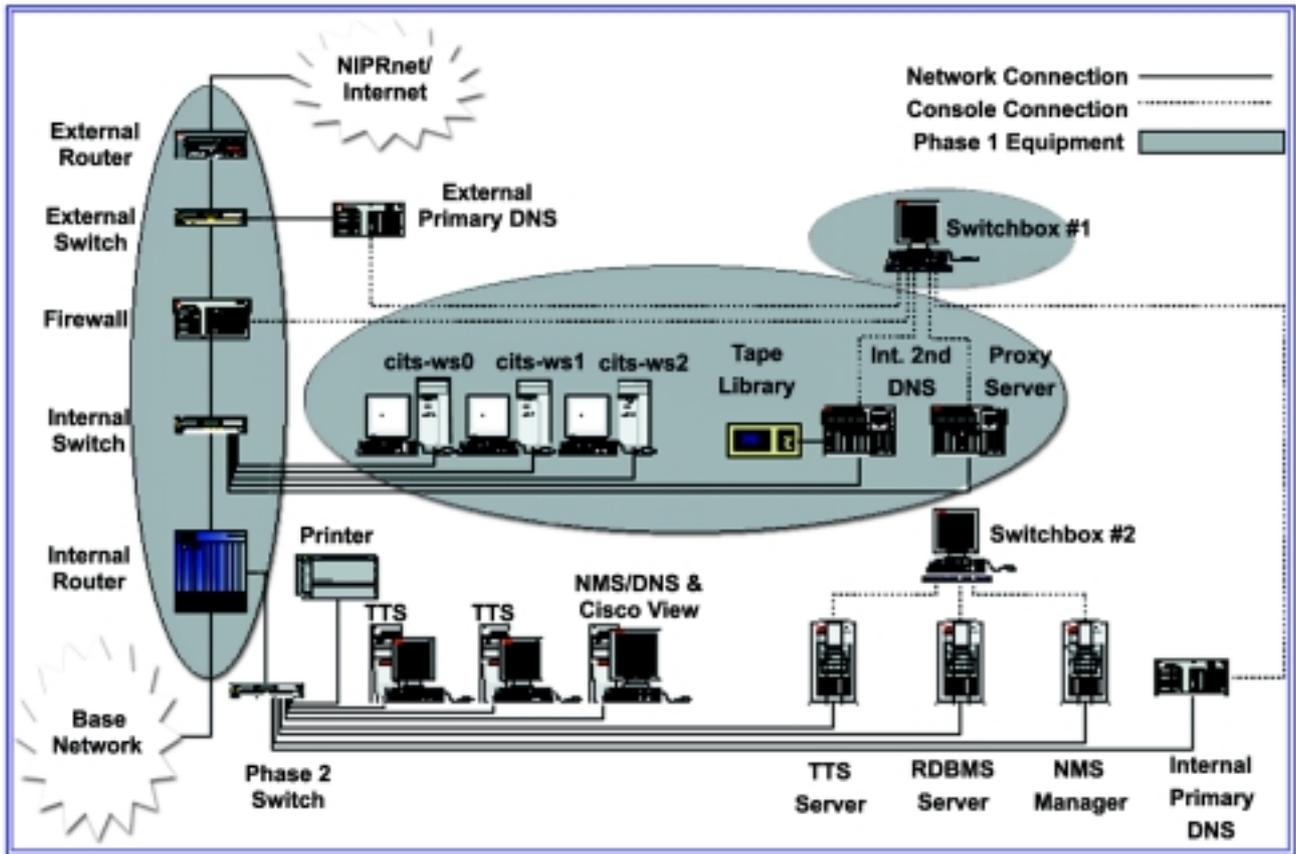
Second, it includes an upgraded and enhanced network management system. Third, it includes a Trouble Ticketing System that is integrated with the NMS so that trouble tickets are generated automatically when the NMS determines that a critical device has failed.

Finally, it includes a second firewall to distribute the high volume of e-mail traffic processed by the firewall and provide a degree of redundancy and load distribution.

An additional Network Node Manager management workstation and two TTS workstations are also provided in Phase 2 so that Help Desk staff can accept and process trouble tickets manually or automatically generated when problems arise.

Phase 2 can be implemented with little or no disruption in current operations. As shown in the figure on the next page, a majority of the Phase 2 equipment is located on a new Phase 2 switch that plugs into the internal router creating a new subnet. Once properly configured, the new segment is activated on the internal router and the new services are available.

The TTS is a new service for most bases, so its use



does not affect any legacy systems for such bases. Similarly, IP management services are new and can be implemented with no disruption in current end-user service.

The NMS is an upgrade of the NMS deployed in Phase 1. The new NMS manager will be configured to provide required network management services. Once the new NMS Manager is properly configured, the Phase 1 NMS server will no longer perform this function. Instead, it will become an internal secondary name server and provide backup services as in Phase 1. This transition will be done in a way that does not diminish the existing network management capability.

Legacy internal DNS servers must be reconfigured to direct all queries to the new Internal Primary DNS Server or the alternate Internal Secondary DNS Server when the primary is not responding. However, this transition can be done as time and resources permit. In other words, legacy DNS service will not be disrupted. However, to optimize the performance of DNS, legacy systems should plan to complete the transition at the earliest possible time. The firewall will be configured to accept DNS queries only from the two CITS DNS servers, but not until all DNS servers on the base have had time to reconfigure their server.

For bases that implement the Barrier Reef DNS recommendation, the transition will be done by the installation team with no service disruption to DNS users. Other bases, including those that bypass the

firewall for DNS service, may require significant preparation before Phase 2.

Phase 2 training occurs between the site survey and installation cycle. A "regional" training concept was selected to optimize training effectiveness within program resources. However, some base locations do not allow for regionalization; therefore, those bases will receive individual on-site training. Regional site groupings will vary from 2 to 6 bases per region. Training is conducted by qualified instructors in a structured, classroom environment with dedicated training equipment, to remove the risk of training on a "live" system.

Each trainee is taught how to perform their NCC duties using the Phase 2 tools, and how to manage and sustain the system. They are also given an introduction to the software and hardware configuration. Each group will attend a three to four week modularized training session, including HP OpenView (three days), DNS (five days), Trouble Ticketing (four days), and in CY99, Sidewinder Firewall (three days). The modular design of the classes allows unit Commanders to send the appropriate trainee to the appropriate class, based on the trainee's duty position.

Phase 3 deployment will begin upon completion of Phase 2, anticipated for Spring 2001. This phase consolidates base remote access with centralized management and authentication, provides full functionality for fault, performance, and configuration management; and

# Information Assurance requires force protection

By Gene Zuratynsky  
*Air Force  
Communications Agency  
Scott Air Force Base, Ill.*



As a communications and information professional as well as a security forces Reserve member, I have a unique perspective on the issue of information assurance and force protection.

Air Force Executive Guidance in October 1996 promoted force protection as a key to mission success. Force protection is more a cross-functional issue than just the traditional law enforcement aspect most people are familiar with. It has led to an Air Staff level working group which brought together the civil engineer, medical, and comm communities as well as others to work force protection issues in addition to establishing a Force Protection Battlelab in 1997.

So what does force protection have to do with information assurance — it has everything to do with IA. Since we must protect the information as well as the systems the information rides on, we must think in terms of physical security, not just cyber security.

Most people tend to focus on protecting our information from the hacker that attacks via electronic means, but the traditional terrorist with a bomb can be just as detrimental. And don't forget the human impact to the mission, if deaths are involved.

Several things can be done during these periods of continuous increased security awareness:

- ❑ Make sure people are aware of what the current THREATCON is and why, if you are a supervisor.
  - ❑ Make sure you know what your responsibilities are under the current THREATCON.
  - ❑ Secure buildings, rooms, and storage areas not in use and increase security/entry checks for those facilities in use as applicable.
  - ❑ Review all contingency plans (e.g., Continuity of Operations Plans, evacuation plans, etc.).
  - ❑ Test contingency plans to make sure they work.
  - ❑ Be alert for suspicious vehicles and individuals on base and around your facilities. Report such things to your local base security forces.
  - ❑ Be alert for abandoned vehicles, parcels, suitcases, or unusual activity. Report such things to your local base security forces.
  - ❑ Key personnel should vary travel routes, departures, and arrival times unpredictability is the key.
  - ❑ And above all else DON'T GET COMPLACENT.
- If you have any questions, get with your experts -- the Air Force Security Forces.
- The bottom line: What good is information if it is not available because it was located in a destroyed building?

- \* Make sure people are aware of what the current THREATCON is and why, if you are a supervisor.
- \* Make sure you know what your responsibilities are under the current THREATCON.
- \* Secure buildings, rooms, and storage areas not in use and increase security/entry checks for those facilities in use as applicable.
- \* Review all contingency plans (e.g., Continuity of Operations Plans, evacuation plans, etc.).
- \* Test contingency plans to make sure they work.
- \* Be alert for suspicious vehicles and individuals on base and around your facilities. Report such things to your local base security forces.
- \* Be alert for abandoned vehicles, parcels, suitcases, or unusual activity. Report such things to your local base security forces.
- \* Key personnel should vary travel routes, departures, and arrival times unpredictability is the key.
- \* And above all else DON'T GET COMPLACENT.

# Common Sense can ensure info security

By 2nd Lt. Reese Frederickson  
690th ISS/PI, Kelly AFB, Texas

Being a member of an information assurance element, I see many situations where a little common sense would ensure basic information security. However, many of us fail to board the common sense train. To keep you on track, I will discuss situations where common sense should apply, but usually does not.

## Prisoners of Government Instructions

I hear many conversations along the following lines: "What AFI tells me how many times I should scan my system for viruses?" asks one of our customers.

"When was the last time you scanned your system?" I ask.

"A while ago, but I need an AFI to tell me when I should do it," he replies.

"I'm glad you called, because AFI (I use a random number like my zip code) says you must scan your system today, and every three weeks after today," I tell him while trying to conceal my laughter.

"I've never heard of that AFI."

"It's the AFI that comes after the one that tells you not to get hit by cars when crossing the street."

"Great! I'm glad I called, or I would have missed the day."

Actually, I'm more truthful in my answers, but the point is that on issues such as virus scanning, common sense should indicate to you that viruses are a computer security threat, and that actions should be taken whenever possible to minimize this threat. You should not need an AFI or some equivalent instruction to guide you on simple computer security issues. For example, do you need an AFI to tell you not to use higher classified storage media in lower classified machines? Do you need an AFI to tell you not to post classified data on unclassified web pages? Do you need an AFI to tell you not to leave your machine unprotected when you are away from your desk? Do you need an AFI to tell you not to pick a password that can be easily guessed? There are many more questions like these, but I would hope the answers are a confident "no."

## Software: The Almighty Solution

I think many people in the Air Force believe that software has infallible powers when applied to computer security. Consider the following conversation:

"There's something wrong with my computer. It is running much slower, suddenly has no memory space, and it won't let me save Word documents," says a worried customer.

"It could be many things, but it sounds like a virus has invaded your system," I say.

"That's not possible because I scanned my system with the latest virus scanner, and nothing was there," he replies.

"That's right," I say, "because anti-virus software companies write all the viruses, and that ensures the latest scan engine will pick up new viruses."

"Really! Those crooks!"

"No, I was joking. I think you missed my point," I say.

"Uh ... I'll have to think about that."

Anti-virus software does not eradicate all viruses "in the wild." Do not assume that strange behavior from your computer is the result of other factors because your anti-virus software did not catch anything.

Remember that software is not perfect. Humans write it, and humans are not perfect. If you ask any professional software engineer if they've ever written an error-free program, he/she will usually laugh at you.

Another point I want to make is that software does not replace human intelligence. Use some common sense when working with software. Also, consider other approaches that may yield more secure results than using software. For example, originate unclassified documents on unclassified machines; this will save you the headache of moving documents to a lower system.

## The Classic OPSEC

I will not mention much on this category, since we all should have been briefed on operations security at least once. Do you need someone to remind you not to write down your password and place it in open view? If you do, send me your address, and I will send one of your coworkers a rubber mallet along with instructions to hit you on the head three times. You get the picture: I hope common sense leads you in the right direction.

## Not Everyone Is Computer Literate

When you work in the communications environment, you can become frustrated by non-technical people. Some comm squadrons receive questions like "where do I put the stamp on my email?" You wonder if these people have any common sense. However they may think you lack common sense if you attempted to do their jobs. You would want them to be patient with you, so be patient with them. I've seen a lot of security incidents happen because someone became too frustrated with an individual to explain proper computer security, which later resulted in a security violation. Although the arguments above are exaggerated, they are intended to make a point. I hope some of the arguments have made you realize that common sense should play an important part in your daily information assurance habits.



# How, why DMS uses Public Key cryptography

By Bert Whitlow  
*Air Force Communications Agency*

Before discussing the details of how public key cryptography is used by the Defense Message System, it seems appropriate to review the requirements that are fulfilled by DMS cryptographic services. Change 2 (Oct. 1, 1997) to the Multicommand Required Operational Capability 3-88, "The Defense Message System", includes the following requirements:

- a. confidentiality/security (prevention of unauthorized access to the information contained within the message);
- b. sender authentication (verification of the sender's identity); and
- c. integrity (assurance that the received message is the same as what was sent).

All of these requirements are achieved by the use of digital signature and encryption with a FORTEZZA® card. The FORTEZZA® card is a tamper-resistant hardware token which stores the X.509 certificate identity of the holder. This identity comprises the "private" portion of the public/private key pair used in public key, or asymmetric, encryption.

## Symmetric vs. Asymmetric Key

Historically, encryption and decryption has been accomplished by the use of symmetric key pairs. This means that the key used to decrypt the message is the same as the key used to encrypt it. Symmetric key cryptography can be extremely powerful when sufficient key lengths are used, but it requires that the sender and recipient both have the same key. The key should only be used once or for a limited time, so that the enemy or unauthorized personnel cannot "crack" the key used in a previous message and apply it to the current mes-

sage. This is a challenging key distribution and synchronization problem, since it is absolutely essential that the sender and recipient are using the same key at the same time.

## Encryption using Public Key Cryptography

Public/private key pairs are asymmetric keys that are mathematically related in such a way that information encrypted with one key can only be decrypted using the other key. The advantage to this method is that one key (the public key) can be posted in a database or repository that is readily accessible to all authorized personnel, while the other (private) key can be maintained within the control of the user. The repository for public key information is typically called the directory. In DMS terminology, this repository is referred to as the Directory Information Base, or DIB. The DIB includes not only the public key for each user entity, but the X.500 address that uniquely identifies that entity.

The primary drawback of asymmetric keys is that they are computationally much more difficult to handle than symmetric keys. This slows down both the encryption and decryption processes, which are performed at the client workstation. This problem is alleviated by using a symmetric key, referred to as the Message Encryption Key for encryption and decryption of the message body. The MEK is then encrypted using the recipient's public key. The MEK is a random number generated by the sending unit that is used only once. The public/private key pair may be used over and over again until the user's certificate expires or it is revoked for security reasons.

This combination of symmetric/asymmetric cryptography takes advantage of the speed of symmetric key cryptography for encrypting and decrypting the bulk of the information to be transmitted, with the added security and accessibility of the public/private key pairs.

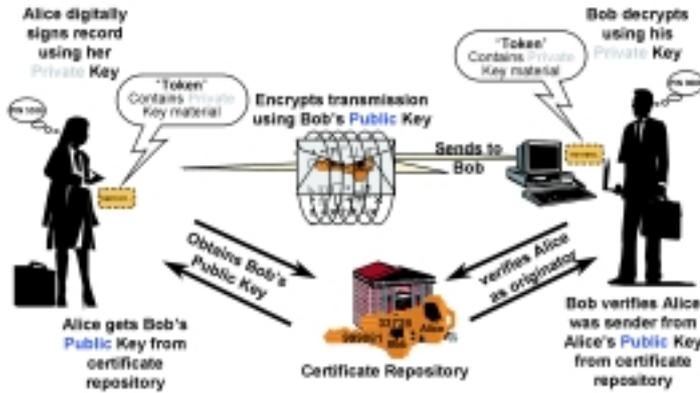
## Digital Signature

The public/private key pairs are also used to verify both the sender's identity and to demonstrate that the message has not been altered to all recipients. This is accomplished by computing a message digest (commonly referred to as a "hash"), that is unique to the message being sent. The message digest is then encrypted using the sender's private key. The recipient client then decrypts the message digest using the sender's public key. If the digest decrypted with the sender's public key matches the digest of the message body decrypted with the recipient's private key, then

## PKI Key Pairs



## Digital Signature & Encryption



the identity of the sender and the integrity of the message are both verified.

### Public Key Infrastructure

One of the most difficult challenges associated with cryptographic services based on a public/private key system is maintaining the integrity of the user's certificate information. As users move to new jobs or are replaced through attrition, their certificates must be "revoked" and new certificates issued. The identity of each user must also be positively verified to ensure the integrity of the certificate issued to that user is not compromised.

Since DMS is a Command and Control system which will replace AUTODIN as the record message system for DOD, a high level of assurance that the certificate system has not been compromised is essential. The high assurance Public Key Infrastructure being fielded to support DMS consists of a hierarchical structure of Certificate Authorities, starting with the Policy Creation Authority at the National Security Agency.

Each CA has a certificate that is signed by the next higher level CA. This certificate establishes the credentials of that CA itself, and is in turn used to sign the certificate of the next lower level CA, on down to the CA Workstation located at the base or site level. Typically one or more CAWs are located at each fixed base and will be deployed in theater when tactical DMS matures. The CAW is used to generate a public/private key pair for each user that is registered into the system. The certificate itself is "signed" by the CA, which positively verifies the validity of the certificate.

The public key is posted to the X.509 directory, while the private key is "burned" onto a FORTEZZA© card. Users are registered through an X.509 certificate request, and the cards are burned according to the privileges and other information on the certificate request. Each organization assigns an Organizational Registration Authority, who is responsible for processing the X.509 certificate request forms and distributing the FORTEZZA© cards once they are programmed. Each

FORTEZZA© card has a unique Personal Identification Number for protection against compromise of a lost or stolen card. Positive control of the card and PIN must be maintained, and each user who receives a card also receives training on proper handling and storage procedures.

### Medium Assurance PKI

Not all users need high assurance protection of messages. There is also an initiative underway to provide a medium assurance level PKI that is based on Commercial-Off-The-Shelf products. The medium assurance PKI is being tested by a pilot trial for the DOD Travel System. Medium assurance certificates will be used to protect Privacy Act information and financial transactions involved with travel of DOD personnel. It is expected that the medium assurance PKI will eventually merge with the current high assurance PKI, at least at the base level. Medium assurance certificates will have applicability to messaging for individual e-mail users and non-critical organizational messaging.

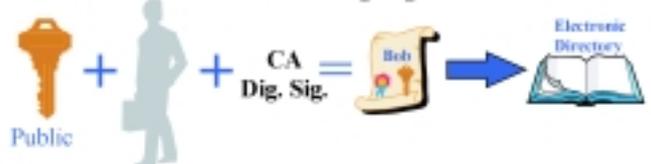
The initial implementation of DMS provides the security services that are required for Command and Control messaging by using a prudent mix of public key cryptography and symmetric key cryptography. Ongoing efforts within the DOD to leverage the existing high assurance PKI for medium assurance applications will ultimately result in a less costly, sustainable PKI for both medium and high assurance applications. DMS is an evolutionary program, and will become more capable with future releases that are planned for FY01 and beyond. The release that will allow most users to transition from AUTODIN to DMS is Release 3.0, which will implement ACP 120 (caveat messages) with an improved Message Security Protocol which will allow for compartmentalization of messages to only authorized recipients. The final step in the transition to DMS will occur when both DMS and the underlying transport infrastructure are capable of ruthless preemption for Emergency Action Messages. This is expected to occur in the FY03 timeframe.

## PKI Concepts

### MATCHING PUBLIC/PRIVATE KEY PAIRS:



### PUBLIC KEY + NAME + CA Dig. Sig. = CERTIFICATE



# Network security – everyone’s issue

By 2nd Lt. David Neuman

83rd Communications Squadron, Langley AFB, Va.

In 1986, as an airman working in a small communications detachment, my shop received its first personal computer – the first one on the base. It was a Z-150, no hard drive, we had to boot off a 5¼ inch floppy drive and put another disk in to use DOS based Wordstar word processing software. We were still doing performance and other reports on a typewriter, and very few systems were accessible from the user level.

Today there’s virtually no aspect of Air Force operations that information technology doesn’t touch. Everything from the cash registers in the dining facilities to the exploitation of satellite pictures to put bombs on target. However, proliferation of the Internet and the low cost of technology have become a threat to our Information Superiority.

Whether you’re a user, programmer, system administrator, or program manager you must be conscious of the need to protect our networks and the systems riding on them. Everyone has a responsibility to understand the implications of poor security and the importance of the information resources we have at our disposal.

Network Control Centers and Wing Information Protection offices are, and continue to be, heavily engaged in educating our people on good security practices. The user who believes surfing the web to get the latest sports scores isn’t hurting anything is wrong.

Many of our mission critical systems share common mediums to communicate. You may be sharing the same path as a system being used to deliver information on air refueling schedules, personnel promotions, or directives from higher headquarters.

Network Defenders in the ACC Network Operations and Security Center see thousands of unauthorized intrusion attempts across the command. While they and the NCCs stand vigilant to detect and defend our network systems from unauthorized and unlawful intrusions they cannot succeed without the help of all who use information systems. Users must be aware of how to protect their systems and what to do when anomalies occur.

We all must follow guidance and directives on password and virus protection, software patches, and directives from the Air Force Computer Emergency Response Team. Failure to do so can have catastrophic results not only for your system, but other systems on your network.

A hacker will typically use a poorly protected host as a staging ground to collect information, passwords, or other infrastructure data to exploit more secured, and possibly critical hosts. Bottom line, a single poorly protected host can present a serious risk to others on your network or networks at other bases. Users or administrators who have questions about information security should contact their Wing Information Protection Office or NCC.

## Leaders discuss tools behind network management and information assurance

SCOTT AFB, Ill. — The Air Force’s communications and information leaders understand the important role that enterprise management tools play in maintaining networks, both for information security and for operational availability.

The leaders immersed themselves in issues concerning use of network management and information assurance tools available to Air Force network specialists during a Network Management and Information Assurance Tool Immersion Day in conjunction with the AF Information Technology Conference in Montgomery, Ala., last fall.

“We all need to be on a common level of understanding about the tools deployed to our bases,” said Lt. Gen. William Donahue, Air Force director of communications and in-

formation, who hosted the meeting. The Electronic Systems Center, Hanscom AFB, Mass., provided the technical portion of the program, giving demonstrations on the capabilities of our current network tools.

“This in-depth introduction to network management and base information protection tools was designed to provide our leaders with valuable insight into the capabilities of current tools and give them a first-hand look at how these tools can meet network management and information assurance needs,” said Col. Gil Hawk, commander of the Air Force Communications Agency, Scott AFB, Ill.

The agenda included briefings, system demonstrations, and open discussions. Topics included Enterprise Management System require-

ments, tools for securing, organizing and controlling base networks, and a look at the way ahead.

“The ability to get the right information to the right person at the right time and in the right format requires a high level of interoperability for command, control, communications, computers, and intelligence systems among all components of DOD and the joint forces. Networks are critical enablers to achieving this interoperability and providing the needed information on demand,” said Hawk. “We must view our networks as critical weapon systems and have the procedures and tools in place to manage them professionally.” (*Courtesy Air Force Communications Agency Public Affairs*)

# Public versus limited web pages

By Senior Master Sgt.

**Chris Hedge**

*Air Force Communications Agency  
Scott AFB, Ill.*

In today's electronic information-dominated environment, there are still many Internet wanderers who are not fully aware of the differences between public and limited (restricted) web sites and the potential security risks they present. Public web sites are accessible to anyone with Internet access, including our enemies. Limited access web sites contain safeguards that limit access to specific individuals or groups, such as military or other government organizations.

Air Force installations are required to provide certain categories of information to the public and public access web sites serve this purpose well. These public accessible sites allow organizations/installations to quickly make releasable information available for public consumption to satisfy Public Affairs, Freedom of Information Act, and other legal/mission requirements. Although public web servers offer this convenience, they also impose critical information assurance con-

cerns.

Too often, information providers make information available to the public without obtaining proper release authority and risk operational security. AFI 33-129, Transmission of Information Via the Internet, outlines specific requirements for making information available to the public. This publication explains that these pages are intended for viewing by the **general public** and information placed on these sites should not adversely affect national security or threaten the safety or privacy of Air Force members or civilian employees. In addition, local procedures must be followed to ensure information destined for the general public is reviewed by Public Affairs, Legal, and Privacy Act/FOIA offices before it's released.

Information posted on Air Force web sites is cleared for release using the same procedures in effect for clearing and approving information for release in hard copy format. When we release information to the public in any form, it's basically considered a FOIA release and requires release approval from the functional communities and appropriate review from the Legal Office, FOIA

Officer, and often a Public Affairs representative. When information is added to limited access web sites, access controls and/or encryption is necessary to protect the information from the public and other restricted parties. OPRs for limited access web pages are responsible for obtaining appropriate coordination and release approval to meet all DOD and Air Force requirements for safeguarding information that could risk operational security.

Each command/installation delegates authority to specific individuals/offices for releasing information via Air Force web sites. Information owners, web server administrators, and web page maintainers must ensure information is properly coordinated with affected agencies and release authorities.

In addition, AFI 33-129, para 7.5., requires web page OPRs to document this coordination in "Internet Release Packages" and maintain these packages in office files areas until the information is removed from the web IAW AFMAN 37-139, Table 37-18, Rule 17.

The OPR is accountable in the event of unauthorized disclosure of limited access information.

## *AFCA to develop guidance on Internet use*

By Senior Master Sgt. **Chris Hedge**

*Air Force Communications Agency*

There have been many questions lately concerning the use of the Internet for non-mission related purposes. Air Force Instruction 33-129, para 3.6., establishes the basis for commanders and supervisors to allow government employees to use the Internet for morale purposes.

Basically, members may be permitted to use the Internet for authorized legal and ethical purposes that are determined to be in the best interest of the Air Force.

This type of use must not interfere with performance of official duties and serve a legitimate Air Force interest such as notifying family of travel changes while on TDY, communications from place of duty required during duty hours, or morale purposes if stationed for an extended period away from home. But most of the questions that have been presented recently have focused on family members' access to military networks for non-mission related purposes.

Many family members seek access to the Internet through Family Support Centers, base libraries, or Department of Defense Dependents' Schools for students attending DOD school systems. The Air Force Communications Agency is developing specific guidelines to further govern the use of the military networks for these purposes and will incorporate a more comprehensive policy into a forthcoming revision to AFI 33-129.

In the interim, the DOD and Air Force policy is to make use of commercial Internet service providers to supply this service to Air Force family members. Network security must continue to be the Air Force's primary concern, while realizing and improving necessary support activities for family members of our Air Force employees. Until comprehensive, alternate avenues are adopted to support non-mission related Internet access, the Air Force will continue to rely on commercial sources of Internet access to facilitate morale and education programs for Air Force family members.

# As interconnectivity grows so does concern for operations security

The world has experienced a rapid integration of information processes and information technology. In the process, the national security posture of the United States has become increasingly dependent on the defense, national and the larger global information infrastructure. These information infrastructures, which consist of information, information systems, networks, and technology, represent worthwhile targets in an increasingly unbalanced threat environment.

Within this global infrastructure lies a medley of interconnectivity which is growing at a phenomenal rate all the time. This interconnectivity, when coupled with search engines and information compilation algorithms, provides a single user the ability to aggregate, analyze, and build new levels of understanding from unclassified sources. As such, the information provided on publicly accessible Web sites is an OPSEC concern.

One way of viewing the information infrastructure is in terms of its basic components--those necessary for transporting the information; the information itself; the means for creating, gathering, and processing data to obtain information, and the storage of the data and information.

Another way of viewing the information infrastructure is as a collection of networks and services such as the Internet, public telephone and data networks, financial networks and services, etc. And still another way of viewing the information infrastructure is in terms of the various domains it serves. These infrastructure domains can contain vast amounts of sensitive but unclassified information.

From an OPSEC viewpoint, when you combine these infrastructure components, networks and services, and domains, you can recognize the vast resources of information available to the public and the adversary and see how the potential for inadvertent or unauthorized disclosure of sensitive information continues to grow.

Given the increasing dependence of our national and economic security upon the information infrastructure, it is essential we apply good OPSEC procedures within our organizations. As such, risk assessment and risk management become critical factors in evaluating publicly accessible Web site information.

The worldwide connection of computer local area networks and wide area networks such as the NIPRNET makes access to defense information from anywhere in the world relatively easy. Separation between the NIPRNET and the WWW is ambiguous, and occasion-

ally these networks may be indistinguishable to Web page administrators.

Web pages intended for internal DOD use should not be made available on the NIPRNET without appropriate access control, as this information is likely to be accessible to non-DOD users. Consequently, OPSEC and information security concerns arise. This requires a union of information security (COMPUSEC and COMSEC) tools and the OPSEC process at the activity level. Activity webmasters, page maintainers, subject matter experts, and OPSEC personnel must develop a disciplined review of all information posted to their locally generated Web sites. This must be done to protect sensitive unclassified and classified information while recognizing the importance of making available timely and accurate information to the intended DOD audiences, the public, Congress, and the news media.

Evaluation of activity information provided on the NIPRNET and publicly accessible Web sites on the Internet should follow current OPSEC methodology:

- \* identify information access points and evaluate their importance to activity operations
- \* determine the critical information for the activity's operations and plans, and do not place information that would

not be of interest or use to the general public on a public access page

- \* determine the threat and assume any potential adversary has access and knows how to search the net
- \* determine the vulnerabilities and know how well Web pages are protected (hacker is generally the INFOSEC threat, and the search engine and browser are generally the OPSEC threat)
- \* assess the risk and determine what protection should be applied to minimize potential loss of critical information and what is the impact on operations and operations support
- \* apply protection by combining information security and OPSEC tools to minimize information loss and vulnerability.

When applying the OPSEC process to information posted to Web sites, the activity also needs to evaluate subject data with regard to the time factor. With today's technology, a single user can connect to the Web and use varying search engines, browsers, and certain aggregation methods to develop a composite of informa-



# Defending a new battlefield ... cyberspace

By Capt. Shawna Wimpy  
Air Force Information Warfare Center  
Kelly AFB, Texas

Why did the Secretary of Defense, ABC News, and Hollywood moviemakers visit San Antonio, Texas? Not to see the Alamo or the famous Riverwalk; rather, to see how the Air Force is defending a new battlefield ... cyberspace.

Cyberspace ... a construct that catches the imagination of the lay-person, expert, writer, and movie producer alike with grandiose dreams of fame, wealth, and fortune or fears of isolation, increased vulnerabilities, and "big brother." For our national leaders, cyberspace is the dual-edge sword slashing towards our future, bringing the promise of great advances and the exposure to new threats worldwide.

The Air Force Information Warfare Center, a subordinate element of Air Intelligence Agency, is the Air Force's expert on the dual edges of cyberspace. The Engineering Analysis Directorate is most familiar with the darker edge of cyberspace ... the edge that brings new threats to Air Force operations.

AFIWC/EA's mission is information protection—protection of the computer systems, networks, and telecommunication switches that the military depends on. To accomplish this mission, AFIWC/EA is divided into three divisions: Air Force Computer Emergency Response Team Operations Division, Countermeasures Division, and Engineering Assessments and Solutions Division.

"Who ya gonna call?!" A phrase made famous by Bill Murray and Dan Aykroyd in the 1984 hit *Ghostbusters*, could be the AFCERT's theme. Who calls the AFCERT? Commanders, system administrators, webmasters, security managers, other Service Computer Emergency Response Teams, MAJCOM Network Operations and Security Centers, Regional Information Protection Centers, and anyone else who identifies suspicious activity on Air Force computer systems and networks.

The AFCERT is the Air Force's response force that isolates and contains suspicious or intrusive activity on the networks. As the operational unit for enterprise-level information protection, the AFCERT's cyberprotection capabilities monitor Air Force information systems and networks for attack and intrusive activity 365 days a year, 24 hours a day.

Just how big is the AFCERT task? The Air Force's unclassified computer networks support more than 6

billion "computer conversations" annually. Network security monitoring devices are placed at all Air Force bases. These devices whittle the 6 billion number down to several hundred million suspicious connections. Through the use of advanced tools, the several hundred million suspicious connections are further pared down to 1-2 million suspicious transcripts.

With the help of advanced tools, AFCERT analysts evaluate these transcripts or the "electronic conversation" between computers. From this review, several thousand Suspicious Event Reports are generated annually. SERs are issued when AFCERT analysts cannot determine if the activity in the transcripts is legitimate or to warn base personnel when the activity is clearly unauthorized. Once base personnel are contacted and the activity in the transcript is validated as unauthorized, the Air Force opens a new computer security incident.

In 1998, there were 93 computer security incidents that resulted in exploitation of Air Force computer systems and networks or attempts to disrupt the networks and computers. Sixty-one of the 93 incidents involved unauthorized intrusions into Air Force computers and networks. Through Nov. 3, 1999, the AFCERT had detected 46 computer incidents involving intrusions this year.

How does the AFCERT accomplish its mission?—people and tools. The AFCERT depends heavily on a cadre of well-trained computer analysts/cyber warriors. Over half of this cadre are enlisted military personnel in the Communications-Computer and Intelligence Analyst career fields. Civil servants, contractors, and officers round out the cadre—providing guidance and critical skill sets.

Working on the front line to protect military cyberspace from exploitation and attack, these individuals are breaking new ground in the development of computer network defense operations. They are warriors who operate in an ever-changing battlefield, encountering new attacks and threats on a daily basis.

But what about the tools used? Tools bring us to the second division in AFIWC/EA—the Countermeasures Engineering Team. CMET members advance the intrusion detection technology used by the AFCERT and other Department of Defense organizations, develop and prototype solutions for new and emerging vulnerabilities, and research new vulnerabilities and technology.

Sounds good, but what does CMET actually do? In

See **BATTLEFIELD** Page 26

## BATTLEFIELD

*From Page 25*

a nutshell, they respond. Many times they respond with technical countermeasures to control rapidly emerging threats that significantly impact Air Force computers and networks.

On the evening of March 26, 1999, CMET received notice from the AFCERT of a new virus called Melissa. The AFCERT had been gathering information from system administrators on this virus, a virus that ultimately shuts down e-mail servers by overloading the servers with virus-generated e-mails. Within hours of the notification, CMET engineers developed an identification method for Melissa that could be used by the Air Force's intrusion detection system.

Over the weekend, this system "killed" more than 10,000 separate connections carrying the Melissa virus to other DOD computers. Working throughout the night and weekend, CMET developed countermeasures for the virus and worked to validate antivirus products ensuring that, if not already infected, Air Force computer systems would be immune to Melissa.

Because Melissa was written to be fast moving, highly infectious, and not easily detected by commercial network monitoring tools; CMET engineers quickly formed a cadre of experts. Personnel from all three AFIWC/EA divisions and Microsoft engineers formed the cadre of experts. This close-working relationship with Microsoft engineers enabled the Air Force to receive computer fixes to Melissa before they became available to the general public.

By the morning of March 28, CMET had created a web site dedicated to providing countermeasures for stopping the spread of Melissa as well as instructions for cleaning infected servers. Using AFCERT established communications methods, the website's location was distributed to system administrators Air Force wide and shared with our sister services. By the evening of March 29, the website had more than 20,000 hits.

AFIWC/EA's response to Melissa is a model victory for how technical synergy and an established communication process with system administrators, other service's response teams, and commercial experts can contain a DOD-wide computer threat and sustain operations of computer networks. This was the first use of network security monitoring to control the spread of malicious logic on Air Force networks and computers.

But while AFIWC/EA personnel may lead the way, it takes work, hard work, at the base to ensure that Air Force computers and networks are secured. It is the third and last EA division, Engineering Assessments and Solutions Division, that is most familiar with actualities of computer security that local system administrators confront day-in and day-out.

EAS is comprised of different security/assessment teams supporting Air Force operations and the acquisition communities. One of EAS's more dauntless teams

is the Computer Security Engineering Team. The main mission of this team is to perform computer/network vulnerability assessments for commanders. During the first eight months of 1999, CSET members assessed 53 separate Air Force networks and participated in four Air Force/DOD-level exercises.

CSET assessments are generally comprehensive assessments targeting the breadth of resident networks. CSET members test networks remotely and locally. Physical security, system administrative practices, and local computer security training practices are all tested. To accomplish this, CSET members use both technical and non-technical means. One favorite non-technical method of testing is through the use of social engineering.

This method uses a probable story line that tricks users into revealing passwords, user identification, or other pieces of sensitive security data about the local network. For example, beware of the call from a system administrator asking for the boss's password and user identification because "the e-mail system crashed," while YOUR system seems to be working fine...!

CSET members have a "find and fix" mentality that provides commanders with an "honest broker" look at the security of their computers and networks. Additionally, as in the case of social engineering, they check on how good the local personnel are at detecting non-technical attempts at circumventing security features on local computers and networks. CSET members are never bored! And sometimes they face situations that even they could not imagine.

During one assessment, a local security policeman "caught" a CSET member performing vulnerability testing against the local network after normal duty hours. As routine, the member was conducting the assessment in an area of the building not normally used as office space, and with multiple laptops spread around him. As the member attempted to lock the laptop and blacken the screen, the security policeman who ordered him to "leave the laptop and not touch the keyboard," did not favorably interpret the member's actions. Needless to say, the team left well impressed with the local security police awareness of how computer intrusions and attacks can be accomplished by the "trusted insider!"

A second EAS team is the Security Technology Insertion and Test team. This team's primary focus is to infuse security into the acquisition process. STIT delivers their support in three fundamental areas. During the acquisition of information systems, STIT members develop, test, and integrate security solutions to correct system security deficiencies. Next, they perform security product testing in support of new information protection requirements. Finally, they perform vulnerability testing of information systems in support of new/upgraded weapons and C4I efforts.

The third team in EAS concentrates on the emis

See **BATTLEFIELD** Page 28

*January 2000*

# Information Warfare Battlelab wants your innovative ideas

By Maj. Paul Rigney  
*Air Force Information Warfare Center  
Kelly AFB, Texas*

You have a great idea, which could be an innovative solution to an operational need within the realm of information assurance. You know that the corporate Air Force acquisition process takes years to bring good ideas to the warfighter. But you also know that current information technology changes every year to 18 months. Knowing these constraints, what can you do to bring your innovative solution to the operator before the requisite technology makes it obsolete?

Submit your great idea to the Air Force's Information Warfare Battlelab. You and your organization will benefit from new contacts with potential users throughout the demonstration process. Moreover, you will receive recognition for your concept at the Air Force Requirements Oversight Council and the Air Force Board.

The IWB was created to quickly evaluate and demonstrate mature and innovative technologies or techniques that could improve the way the Air Force organizes, trains, and equips. The concepts the battlelab examines must have utility at the operational and tactical level, and could end up influencing Air Force doctrine and tactics. While our long-range vision, Global Engagement, stresses the importance of innovation in the Air Force's future, the IWB also strives to quickly get innovative technologies and shorten the traditional acquisition cycle. The process works with mature technologies, limits each project to 18 months, and provides a short chain of command for quick review and approval.

By the end of October 1999, the Information Warfare Battlelab had received more than 230 submissions. To date 15 have been completed, seven are in demonstration phase and seven have been approved for FY00.

Anyone can submit an idea; while the majority are received from industry, many come from the Air Force and other government organizations.

Concepts address any of the six classic IW activities: electronic warfare, psychological operations, deception, destruction, security measures and information attack. They also address information operations, especially when they lean towards IW more than the

emphasis area of the other battlelabs. To this point, IA proposals have made up a significant portion of IWB submittals totaling 35 percent of the concepts received.

The selection process begins with receipt of an idea. Typically, an idea comes as a three-page white paper in response to the Broad Area Announcement. Other submittals are e-mails or letters. While no submissions are rejected based on their form or content, those that follow the suggestions in the BAA or the battlelab's web site are easier to evaluate, tend to be more complete, and probably have a better chance of success. The IW

Battlelab recommends contacting them prior to submittal to ensure the idea fits within the battlelab's charter and that the write-up contains all the information the battlelab needs.

To be selected, a concept must be mature, able to be demonstrated in less than 18 months, affordable, and have strong military utility. The Battlelabs are not authorized to fund research and development projects, but are given operations and maintenance funds to complete the operational demonstrations. This leads to the requirement for mature concepts. The 18 month time limit on initial funding to briefing the Air

Force Requirements Oversight Council assures that promising concepts will transition to the forces as soon as possible.

Typical demonstrations can range from a software demonstration in an AFIOC computer facility to field exercises such as Green Flag.

After the demonstration, the battlelab prepares an after-action report and briefing for the AFROC. The briefing closes out the initiative and must occur within the 18 month limit. If the initiative has been a success, a transition plan is also built by the Battlelab and the recommended users. The briefing may also be given to the Air Force Board at the AFROC's request. The battlelab's charter ends after the AFROC or Air Force Board briefing, and the follow-on transition process worked. A demonstrated system might become an acquisition program or part of an advanced concept technology demonstration.

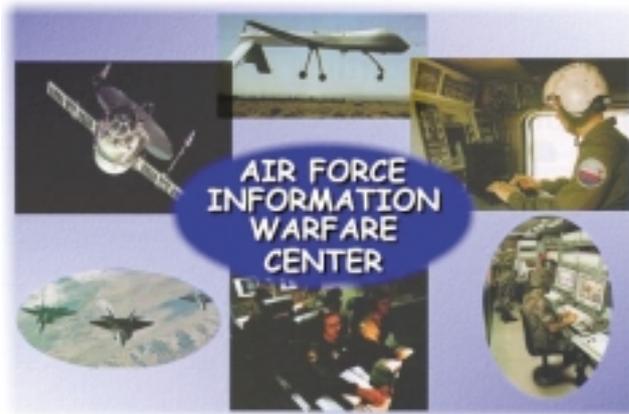
The battlelab's first few initiatives dealt directly with the information needs of the warfighter. IW Reachback used satellite communications to supply for



See **BATTLELAB** Page 28

*intercom*

27



## BATTLELAB

From Page 27

ward units, without existing secure communications, a means of receiving sensitive IW information. Several operational units across DOD are using the system and integrating it into their other communications suites. CyberWarrior was a three-dimensional visualization tool that allowed the user to view databases or structures in a links and nodes format from any angle. By clicking on elements of the structure, additional detail can be obtained. Hierarchy of the network and potential choke points can be assessed from visual inspection.

A highly successful demonstration, which had a direct bearing on IA, was Network Early Warning System. This initiative demonstrated algorithms that evaluate traffic into and out of an Air Force base network to predict impending network attacks.

Another IA initiative, which complements NEWS, is Network Attack Visualization. NAV automatically correlates geographically and temporally separate events that might indicate the clear trail of a network attack. To make it easier for the operator to understand and visualize the results, the software displays its output in a 2-D cluster (galaxy) or a 3-D topographical format. Local clusters and high peaks indicate relationships among similar events.

The battlelab recently received several new IA ideas. For example,

proposals under review include: tools to detect and analyze information in altered data files; special security for system administrators; tools which may help recover computer resources that have been hacked.

A variety of other projects are underway covering the other IW activity areas. A miniaturized GPS jammer was demonstrated to complement other recent technologies. Signal Analysis Mapping demonstrated an anomaly prediction system that improves discrimination between threat and non-threat radio frequency emitters, improving the efficiency of EW systems in hostile environments.

Pulse Doppler Identification proved enhancements to aircraft radar identification systems could provide additional information for target recognition. Software Agents for Opsec demonstrated software to collect, analyze, and correlate open-source internet information on possible operations security problems.

Those are just a few of the innovative ideas the battlelab has received and demonstrated. The battlelab's challenges for the future include expanding its participation in joint exercises and experiments while at the same time focusing on initiatives that will make our forces more effective and lethal.

The battlelab invites you to become a participant in improving our forces, by sending them your ideas. You can find out more at [www.afiw.c.aia.af.mil/who/directors/bl\\_def.htm](http://www.afiw.c.aia.af.mil/who/directors/bl_def.htm).

## OPSEC

From Page 24

tion that surpasses traditional knowledge levels.

As such, the user must determine the value of information with regards to time. Certain data such as unit history, emblems, command affiliation, etc. will have less time criticality than will deployment orders for exercises or real world operations. The value of information may also change over time. For example, the specifics of post-deployment preparations should not be posted to a publicly accessible Web site before the deployment.

Once in theater, unit types, number of personnel and equipment will become public knowledge over time, decreasing the sensitivity of the data. Subsequently, the same information will again become sensitive as re-deployment dates and unit withdrawal specifics are planned.

OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other sensitive activities. OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. In the past, OPSEC has focused on activities that might be seen by a human observer, a satellite, a radio intercept operator, or the news.

The old threats have not gone away, but there is a new area of concern that OPSEC officers and planners must consider the Internet. A disciplined approach to information security procedures in conjunction with the OPSEC process will ensure that sensitive information is properly safeguarded. *(This article is an excerpt from Deputy Secretary of Defense Memorandum, Web Site Administration Policies & Procedures, Nov. 28)*

# AFCA holds Info Protect seminar

By Master Sgt. Ed Goreczny  
Air Force Communications Agency  
Scott AFB, Ill.

The Air Force Communications Agency's Information Protection Seminar covers all aspects of Information Assurance/Information Protection. Briefing topics range from well-established procedures, to what the future is bringing — how technology is changing security, as we know it. The overall Information Protection Seminar objective is to help attendees understand current/future IP directives, disciplines, and responsibilities; including threats and associated risks.

The seminar is an open-forum, subject-intensive venue. It is an awareness seminar that provides attendees with what they need to know to manage offices working the various security disciplines. It is not a 'how-to' class detailing each of the security disciplines. The details of the specific disciplines are taught in formal AETC courses. The number of topics and amount of information discussed in the seminar has been described as "staggering" and "brain-numbing."

The subject matter experts who write policy and procedures for the various topics take time away from their normal work to brief at the seminar. This provides the attendees an opportunity to talk directly with the people making or recommending the rules.

A large advantage of the seminar is the interaction between the briefers and the people who attend from all around the globe. This interaction informs the policy-makers about what's going on in the field.

The briefers want to hear what people are doing in the field. They want to know if the policy-makers are doing the right things and the information provided makes sense. The informal atmosphere allows maximum briefers/attendee interaction. Briefers learn as much from attendees as they learn from the briefings.

In addition to the different security programs briefed and discussed, the AFCA Commander shares

his views of information protection and information assurance. This helps people gain senior officer insight into critical initiatives and the impact these initiatives will have on base-level resources, processes, and procedures. He also talks about how Communications and Information strategy is evolving to meet expeditionary aerospace operations needs. He wants everyone to understand the relationship between the AF Communications and Information Center, AFCA, and the MAJCOM/FOA/DRUs, and recognize their roles in achieving Comm and Info strategic objectives.

Some of the topics covered include the Security Awareness Training and Education program; Emissions Management (also called Emission Security); Key Management (Communication Security); Network Protection Policies, Procedures, Rules, and Responsibilities; and Certification and Accreditation of systems. We'll discuss Public Key Infrastructure, Operationalizing and Professionalizing the Network, Combat Information Transfer System, Base Information Protection Tools, and security issues for wireless LANs. Not everyone is intimately involved in all the areas, but as IP/IA people, we need to be familiar with all disciplines and how they contribute to enterprise-wide security.

All the IP seminars have several guest speakers talking about related topics. These topics include Cyber Crime by the OSI and 3C functional issues. AFCA wanted to round out the information provided, show how the IA/IP arena is changing, and why our jobs are so important.

People in the Air Force Information Assurance world interested in attending the IP Seminar should contact their base and MAJCOM training managers. The IP Seminar runs about once a month.

For more information on the Information Protection Seminar held at Scott AFB, please look at our home page at [www.afca.scott.af.mil/seminars/](http://www.afca.scott.af.mil/seminars/) or contact Master Sgt. Ed Goreczny via the seminars office box AFCA-XPFS@scott.af.mil.



## BATTLEFIELD From Page 26

sions security aspect of information protection. EMSEC team members assess and report on secure information processing systems. The Presidential fleet, special operations aircraft, F-22s, and various wing-level command and control systems are some of the more notable systems that this team assesses. Two commercial motor homes have recently

been converted for EMSEC testing purposes. These motor homes crisscross the nation delivering team members and tools necessary to test systems in operational settings and lab settings.

So, who is called when "ghosts" have invaded cyberspace and the Air Force requires cyber-defense? When identification of suspicious computer activity is required; when new solutions must be developed for quickly emerging cyber-threats; when an

information system is deemed too important to address security concerns after the Air Force has already bought it; or when your commander needs to know how well-prepared YOU and your computer systems are to meet the cyber challenge? Frequently it is the men and women of the Air Force Information Warfare Center Engineering Analysis Directorate. People who believe they have some of the most exciting and rewarding jobs in the Air Force.

# Singing from the 'same sheet of music' with Joint Technical Architecture - Air Force

By Thomas Sapienza  
Air Force Communications Agency  
Scott AFB, Ill.

Information Assurance is definitely one of the most daunting tasks facing our Air Force. Boundary protection, Virtual Private Network concerns, encryption, viruses, and the list goes on and on. We've all worked solutions to the problem, but unless everyone is singing from the same sheet of music, we'll have disconnects. That "same sheet of music" is the Joint Technical Architecture - Air Force. The intent of this article is to show you how Information Assurance and the JTA-AF have joined hands to bring you, the customer, a means to protect your information.

Let's begin with an overview of what the JTA-AF is. In layman's terms, the JTA-AF contains the standards, recommended products, and guidance surrounding a myriad of areas, such as information transport, information processing, database utilities, multimedia, and, of course, security. Standards in the JTA-AF come in two flavors: mandatory and emerging. Mandatory standards are just that—the Air Force Chief Information Officer, Dr. Lawrence J. Delaney, signed a letter to this effect Aug. 2.

Emerging standards are meant to show you the "road ahead." In other words, it helps you prepare to migrate toward the potential mandatory standard of the future. Recommended products identify vendor products which support our mandatory standards. The reason for recommended products is to promote interoperability and cost of ownership across the Air Force. And, lastly, the JTA-AF also provides guidance. Our latest method of providing guidance comes in the form of Information Technology Infrastructure Architectures.

ITIA's are designed to focus on a specific technology or capability, and break it down into bite-sized chunks. The resulting "chunks" may be standards, products, guidance, or any combination—depending on the focus, maturity of industry solutions, etc. That's JTA-AF 101. To summarize, it's a one-stop-shop to obtain the information you need to ensure interoperability and ease of

implementation.

How does Information Assurance fit into all of this? Protecting our information is the number one priority in our business. That's why the first ITIA we built covers Information Protection, a subset of Information Assurance. The goal of this architecture was to provide a view of the "inside the gate" portion of the Global Information Grid.

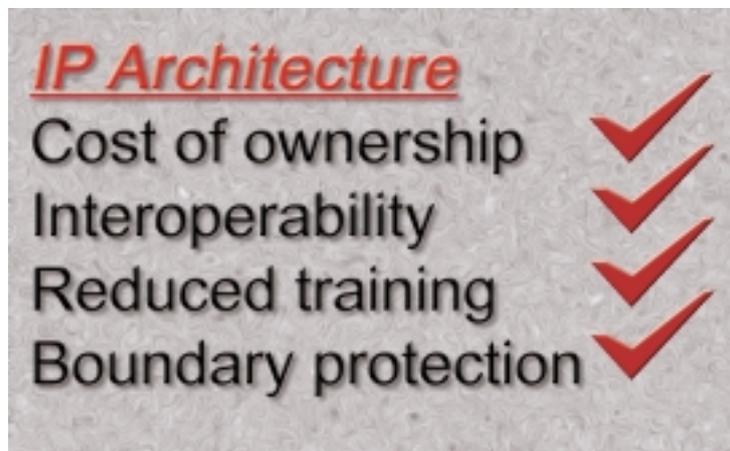
As such, the major categories of boundary protection, internal control, intrusion/misuse detection, access control, access preservation, and encryption were covered. Standards to support all these functions were identified, most of which were already found in the JTA-AF. The others were added to ensure full support for the architecture. Additionally, recommended products resulted from the effort. Toolsets from CITS/BIP, as well as additional security tools found in AFSSI 5009

were all deemed to be viable mechanisms to help ensure Information Protection.

And lastly, guidance is prevalent in the architecture. The working group who spearheaded the effort came to agreement on several issues to help you in setup, configuration, and execution of IP efforts at your installation. Difficult challenges, such as legacy applications running

through firewalls, shunts (bypasses) around the firewall, and applying intrusion detection to ATM traffic were discussed during the working group, with decisions being included in the architecture.

Starting to see the link here? The Information Protection Architecture includes standards, products, and guidance—much like the JTA-AF. The architecture will be voted on by the Configuration Control Board soon. The result will be incorporation of the architecture into Section III of the JTA-AF—the two are indelibly linked—the IP Architecture is a formal part of the JTA-AF, and the JTA-AF provides the vehicle to ensure compliance with the standards contained in the IP Architecture. Cost of ownership—done. Interoperability—done. Reduced personnel training—done. Boundary Protection—optimized. That's just a sampling of the benefits of using the IP Architecture and JTA-AF. If we do, we'll all sing to the same sheet of music ... in harmony!



# Multimedia/visual information products provide info assurance awareness

By Carmen Hensley  
Air Force  
Communications Agency,  
Scott AFB, Ill.

Information and technology overload! The availability of information goes hand in hand with the increasing need for information protection and information assurance at its best. To support the Air Force mission in providing information assurance and security awareness education, training in all forms is a must. So what is available to Department of Defense activities to support education and training requirements.

Traditionally known as audiovisual products, AV productions and interactive multimedia instructional products include videotapes, films and multimedia programs to support organizational, training, and internal information missions. Videotapes and CD-ROMs are current formats of delivery medium to support a wide range of training requirements today.

Videotapes provide a flexibility to an organization's training schedule. Whether it is viewed by one person or a larger target audience, the flexibility is there for video presentation. DOD organizations acquire video products to support training from the Defense Automated Visual Information System/Defense Instructional Technology Information System.

DAVIS/DITIS is a quick and easy online database that allows users to search thousands of multimedia products. The convenience is at your fingertips. Visit the Defense Visual Information website [DODimagery.afis.osd.mil](http://DODimagery.afis.osd.mil) to access information on various subjects to support your organization's training requirements. The database evolves daily with the addition of new products and deletion of old ones. Centrally managed by the Office of Assistant Secretary of Defense Public Affairs, American Forces Information Service, the Defense Visual Information directorate provides central oversight of the information loaded onto the DAVIS/DITIS.

The DAVIS/DITIS provides an on-line ordering capability of products from a Production Identification Number record. The PIN is a primary reference source used to locate a multimedia production record. Once you have located the record, you can order the product by completing the online request form, a single copy of



the product will be shipped at no cost to your organization.

Look in the DAVIS/DITIS to find out what videos or multimedia products have been produced in support of security training and information assurance. The following are the Air Force's top issued video titles for security training: Cyber Strike II, PIN 613046  
Cyber Warriors- Info War, PIN 613641  
Computer Security, Part I

- "Your Name on the Line", PIN 612882

Computer Security, Part 2 - "You are the Key", PIN 613054

Cyber Warriors - Digital Battlefield, PIN 613640

Cyber-Strike, PIN 612703

The PIN is used for record entry in the DAVIS/DITIS. Each service component has a DAVIS/DITIS Data Record Administrator responsible for record entry and updates to the DAVIS/DITIS databases. The Air Force Communications Agency, Multimedia Services Branch, AFCA/GCOV is the Data Record Administrator for Air Force records.

All product records listed in the DAVIS/DITIS are physically inventoried and lifecycle managed by the Joint Visual Information Service Distribution Activity located in Tobyhanna Army Depot, Pa. As the executive agent for replication and distribution activity for all the services, JVISDA provides lifecycle management of all products in supporting initial, supplement distribution and supporting product requests received through the DAVIS/DITIS. JVISDA can support mass quantity distribution for organizations requiring multiple copies of products. The requesting organization must assume JVISDA's replication and distribution costs. If multiple distribution of copies is required, please contact the Air Force distributor at JVISDA, DSN 795-6543, or commercial at (570) 895-6543.

The DAVIS/DITIS and JVISDA are there to support your training needs. They provide a flexible online capability for users to obtain products.

For multimedia production requirement information, visit our Multimedia Services Homepage at: [www.afca.scott.af.mil/multimedia/](http://www.afca.scott.af.mil/multimedia/) or contact the AFCA Multimedia Services Branch at DSN 576-3487/6344, or commercial at (618) 256-xxxx or e-mail: [afcagcov@scott.af.mil](mailto:afcagcov@scott.af.mil).

# Public Key Infrastructure

## learning what it is, is not

By Ron Drumm

*Air Force Communications Agency*

*Scott Air Force Base, Ill.*

### What a PKI is:

A public key infrastructure provides the resources and capabilities necessary for the generation, certification, and distribution of keys for computer applications which require public and private keys to support their information assurance capabilities (digital signatures and data encryption).

Software applications which provide a digital signature (identification and authentication) and/or a privacy (data encryption) capability for communications over open systems such as the non-classified Internet protocol router network or Internet require the use of key material. Key material is used for the generation and authentication of digital signatures and for encryption and decryption of information.

Currently the method for providing key material (e.g., paper key tape and the like) is to send it, via protected means, to each participant of the secure session. To support users in a distributed network, a PKI may be used. In a PKI, a set of two keys is used. One is called the public key and the other is the private key. They are generated and certified in matched pairs. The user's public key is made available to the public by certifying it and posting it on a directory server. A copy of the certificate may also be provided by the user. The certification process assures the authenticity of and binds the user to the key material posted on the public server. The private key is held and protected by the end user.

❖ For digital signature capabilities, the sender's application uses his/her private key to develop a digital signature. The recipient of the information obtains the sender's public key from a directory server and his/her application uses it to verify the digital signature of the sender thus authenticating the sender and the message content.

❖ For data encryption, the sender obtains the public key of the receiver from the directory server and uses it to encrypt the information transmitted to the receiver. The receiver then uses his/her private key to decrypt the message content.

### What the DOD PKI is not:

- ❖ An encryption capability
- ❖ A digital signature capability
- ❖ A source of solutions for encryption or digital signature capabilities
- ❖ Responsible for modifying user applications to use PKI support mechanisms

### Corporate Air Force Responsibilities

Ensure a user registration capability is available to the user community

- ✓ Registration Authority responsibilities reside at Cryptographic Support Group
- ✓ Local Registration Authority responsibilities initially tasked by AFCIC to reside in the Wing Information Assurance/Information Protection Offices
- ✓ AF LRA training is scheduled with DISA by requesting through the Air Force PMO. PMO POCs are listed on the AFCA web site.

### User Responsibilities

Users requiring digital signature or encryption capabilities must:

- ✓ Have their applications modified to incorporate encryption or digital signature modules.
- ✓ Ensure encryption modules comply with FIPS 140-1
- ✓ Ensure digital signature modules comply with FIPS 186-1 and FIPS 140-1
- ✓ Ensure application is enabled to be supported by the DOD PKI (PKI enabled)
  - ▶▶ Interface Specification for Developers available from DISA
- ✓ Determine network loading posed by modified applications
- ✓ Ensure applications are compatible with or comply with network Information Protection mechanisms:
  - ▶▶ Firewalls
  - ▶▶ Barrier Reef
  - ▶▶ Secret And Below Interoperability

### Local Registration Authority

A local registration authority is responsible for verifying the identity of and for registering users of the PKI. Since the DOD PKI anticipates issuing only identity certificates, there is no requirement for the LRA to determine an entity's privileges. The LRA ensures that users understand liabilities and responsibilities associated with the possession of a private key and agree to abide by the established rules.

The LRA may also be required to obtain certificates for non-human entities such as components that need cryptographic material and certificates. The LRA must establish the legitimacy of the request and typically will work with an individual responsible for the component. The LRA must report any suspected compromise to the RA who then revokes the affected certificate. The LRA forwards all user registrations to the DOD Certificate Authority where the actual certificate is generated and posted to the directory server.

### The User

The user, or PKI *subscriber*, is the owner of the pri

vate key that is supported by the PKI. A PKI user can be a human or can be a component. When the user is a component, there will be some individual responsible for the operation of the component (e.g., system administrator). In general it is desirable for the user to generate a key pair locally and provide only the public key for obtaining a certificate.

In some circumstances, the user obtains the key pair from the certificate authority server which generates the key pair and the certificate simultaneously. The user is responsible for interacting with the LRA to obtain a certificate. The user must protect the private key from disclosure since failing to do so would allow someone to masquerade as that user. The user must report any suspected loss or compromise of the private keys. The user is responsible for complying with established policy and using private key in accordance with the policy.

Users must ensure their applications requiring PKI support include encryption and digital signature modules which are National Institute of Standards and Technology validated (Federal Information Processing Standard compliant) and that they are developed or modified for compatibility with the DOD PKI. The DOD is in the process of selecting a "smart card" to be called a common access card. This device is to replace the current DOD ID card (military and civilian) as well as include additional features such as the secure storage of a user's PKI certificate private key.

(Point of contact for Air Force PKI direction and guidance is William Meskill at DSN 425-6174. The Lead Command POCs at AFCA are Ron Drumm and Master Sgt. John Bodien at DSN 576-2498/2645).

### Where We Are

The DOD PKI effort was directed by Dr. John Hamre, Deputy Secretary of Defense, and did not require the development of a MNS or ORD. However, an Operational Concept of Employment (as per AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*), was drafted by AFCA, staffed through the major commands and is being revised to include new DOD direction.

To provide support to this effort, an Air Force Program Management Directive #2425 was developed. In it, AFCA is identified as the Air Force Lead Command and the Cryptologic Systems Group (CPSG, now ESC/DIW) the Air Force PMO. The PMD provides all participants with the direction needed to meet DepSecDef mandated schedules. To disseminate Air Force policy and procedures, Air Force Instruction 33-213, *DOD Public Key Infrastructure Management and Use* was developed. Although the majority of the staff work and MAJCOM review is completed, the AFI is on hold until

DepSecDef redirection is received.

To ensure Air Force interests are addressed, AFCA participates in the DOD PKI Working Group meetings and supports the review and development of DOD-level documents such as the DOD PKI Roadmap and X.509 Certificate Policy. The working group sessions bring important service and agency issues to the table with problem areas identified and resolved. The two DOD documents lay out the course for implementing the PKI in the DOD and establishing a standard for certificates to ensure total interoperability within the DOD and with civil and coalition counterparts.

Ensuring all sites receive PKI support is important. Not only are we concerned with the lack of available manpower and the need for additional funding, we are concerned with easing or eliminating the initial workload for registering all AF personnel by October 2001 as mandated by DepSecDef. Our intent is to supplement organic resources with contractor teams and dispatch them to the various Air Force sites (to include the Guard and Reserves). We are also identifying the specific sites which provide Air Force support and also those which require AF support. To date, more than 500 locations have been identified.

Concerned with the additional workload placed on local registration personnel, we have ensured tools are available to support time-consuming user registration tasks. Three tools have been developed to assist Local Registration Authorities to complete user registration; they may choose the one which best fits their situation. The PMO continues to schedule and monitor DISA-provided LRA and Registration Authority training to ensure the appropriate local (base) office receives training to support DOD implementation actions.

Working with our counterparts in the Systems Directorate, we are continually identifying systems and programs requiring Public Key support.

Because of the similarities of the DMS and DOD PKI structures, there are economies of scale which may be achieved through the combination of certain efforts. The PKI and DMS PMOs are exploring ways to capitalize on existing DMS capabilities and infrastructure.

To promote awareness and understanding of PKI efforts, we continue to provide briefings to our Information Protection and Network and Systems seminars. To ensure compliance and understanding by the Air Force program and implementation community, the PMO provides briefings to program and project managers. We've also posted vital information on our PKI home page.

Additional PKI information and descriptions of the various assurance levels (Classes) are available on our web site [www.afca.scott.af.mil/ip/compusec/pki/pki.htm](http://www.afca.scott.af.mil/ip/compusec/pki/pki.htm)



# Firewalls 101 —

## An introduction to protecting the network from an outside network

By Master Sgt.  
Scott Noeldner

Air Force  
Communications Agency  
Scott AFB, Ill.

Most network users in the Air Force have heard the term “firewall” and know it has something to do with computer security, but many don’t know exactly what this means. Also, firewalls are often “blamed” for slowing down the network. (*In layman’s terms a firewall is any one of several ways of protecting one network from outside networks.*)

### Problem

The Internet is a vital and growing network that is changing the way organizations and individuals communicate and do business. The Department of Defense uses the non-classified Internet protocol routing network (NIPRNET) as its primary link to the Internet. However, the Internet suffers from significant and widespread security problems. Air Force users connect to the Internet through NIPRNET, and therefore share many of the same vulnerabilities.

Many government and civilian agencies and organizations have been attacked or probed by intruders, with resultant losses to productivity, reputation, and valuable or sensitive data. In some cases, organizations have had to disconnect networks temporarily, and have invested significant resources in correcting problems with system and network configuration. Sites that are unaware of these problems face a significant risk that they will be attacked by network intruders. Even sites that do observe good security practices face problems with new vulnerabilities in networking software and the persistence of some intruders.

A number of factors have contributed to this state of affairs. The fundamental problem is the Internet was not designed to be very secure, i.e., open access for the purposes of research was the prime consideration at the time the Internet was implemented. However, the phenomenal success of the Internet in combination with the introduction of different types of users, includ-

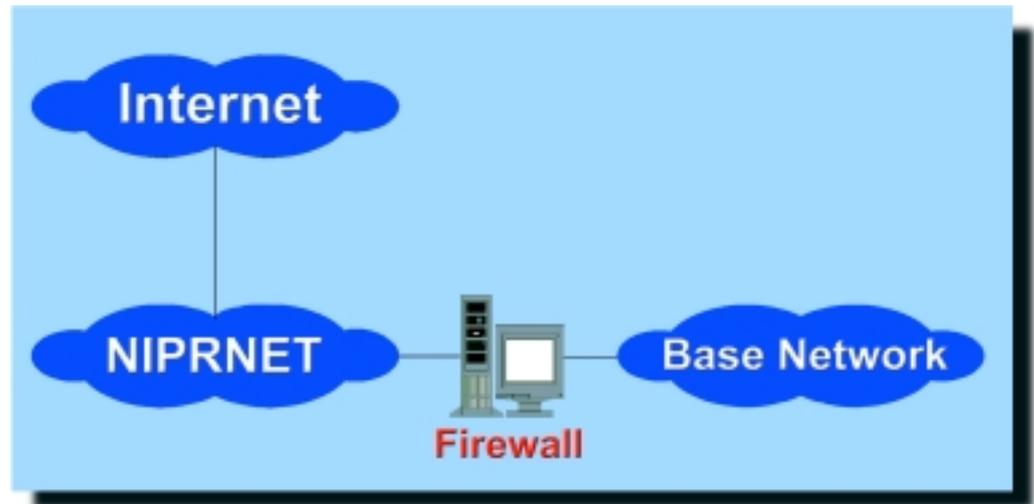


Figure 1: Simple Network Diagram

ing unethical users, has aggravated existing security deficiencies to the extent that wide-open Internet sites risk inevitable break-ins and resultant damages. A combination of political and military factors make the DOD and Air Force networks especially popular with individual and state-sponsored attackers.

### Solution

Fortunately, there are readily available solutions that can be used to improve site security. The Air Force uses the Barrier Reef process to plan and implement network security. This is the electronic equivalent of the *physical* perimeter defense provided on our Air Force bases by our security forces. Barrier Reef is a 12-step process that provides a systematic approach to establishing boundary protection that is coordinated with the overall Air Force network strategy of providing professional, secure network service.

A firewall is one component identified by the Barrier Reef process that has proven highly effective for improving the overall level of site security. (The Barrier Reef process explains the concept of defense in depth, but is beyond the scope of this article. Network security professionals can find additional details on the Air Force Information Protection homepage at [www.afca.scott.af.mil/ip](http://www.afca.scott.af.mil/ip).) A firewall is placed at a base’s central connection to the NIPRNET (Figure 1) and forces all network connections to pass through the gateway where they can be examined and evaluated. The

See FIREWALL next page

# Tools identify weak passwords

By Larry Johns

*Air Force Communications Agency  
Scott AFB, Ill.*

Information Assurance begins with some basic requirements. A key element in controlling access to information systems is the requirement for all users to provide some form of identification. A primary means of doing this is for the user to provide a user ID and password. The password provides the first line of defense for our information systems, and that defense is weakened by poorly constructed passwords.

Air Force requirements for password construction and selection call for passwords to have a minimum of eight alpha-numeric characters (upper and lowercase, and at least one special character). System administrators have the availability of password-cracking tools to identify the use of weak passwords. Unfortunately, these tools are not normally used until the password has been in use for some time.

The Air Force is evaluating the use of a password policy enforcement tool that will check passwords as the user initially enters it into the system. Direct feedback is immediately available to the user when the entered password does not meet the requirements, or when the entered password is listed in the tool's accompanying dictionary.

Password cracking tools typically check the password against a dictionary to determine if a match can be found. In some cases the tool will check variations of the dictionary words by adding a letter or number to the beginning or end. The more sophisticated tools use a combination of the dictionary check and then have the capability to complete an exhaustive attack of the password. Exhaustive attacks involve the submission of as many different password values as possible in the

hopes of finding one or more which are valid. The work factor for someone attempting an exhaustive attack is directly related to the number of possible values, which must be tried for each character of the password.

The following illustrates the increased difficulty of cracking passwords when using properly constructed passwords. Using the 26 letters of the English alphabet in any arbitrary arrangement, the number of possible passwords that can be formed using N letters is 26 to the Nth power. The total number of passwords comprises the password space. Thus, using 5-letter passwords, there would be 26 to the 5th possible combinations, which is equal to 11,881,376. This is fairly easy for a password cracking tool using an exhaustive attack to try all the combinations in a relatively short time. Increasing the password length to eight characters will increase the number of combinations to 208,827,064,576. This significantly increases the time required for the tool to try all the combinations. The addition of upper case letters, 10 numeric digits, and the possibility of 25 or 30 easily inserted special characters will increase the number of combinations to a gazillion or two (more than I can figure or comprehend). This number will significantly increase the time required for the cracking tool to try all the combinations. Still, it's not an impossible task given enough time and computing power, but this should be enough to discourage casual intruders. Adding numerics and special characters also makes it more difficult to discover passwords when checked against a dictionary.

Do your part to help protect our information systems by following the rules for properly constructed passwords.

Air Force password policy is contained in AFMAN 33-223, *Identification and Authentication*.

---

## FIREWALL

*From previous page*

firewall may then restrict access to or from selected systems, or block certain network services, or provide other security features. The base network security policy can be implemented by the firewall to provide access from internal to external systems, but little or no access from external to internal systems.

The access control rules shape the base network security policy. These access control rules are configured in a database called the Access Control List. Each rule determines whether or not a user pro-

gram may open a connection to a network service proxy or a server application on the firewall. The connection request may originate from either the internal base network or outside the base network. A proxy-based firewall acts as a middleman between untrusted external computers and trusted internal computers.

When a network connection is requested, the firewall checks the ACL entries to determine whether to allow or deny the connection. While this process does introduce additional processing of data during transmission, a properly configured firewall should add minimal impact to the overall network response

time. Note: A properly configured firewall significantly improves our network security, but it is still very important to practice safe computing at all host computers, as well as desktop workstations (e.g., up-to-date antivirus software, no modems, current backup).

Our interconnected world has made it necessary to use firewalls as part of Barrier Reef perimeter defense because of the constant threat from would-be attackers. Hopefully the next time you hear the term "firewall," you'll have a better understanding of how they're used in the Air Force.

# Global Information Grid - Air Force allows info to be transmitted to warfighter

By Donald Miller  
Air Force Communications Agency  
Scott AFB, Ill.

Joint Vision 2010 and Air Force Global Engagement identifies information superiority as a key factor of our operations today and into the future. Information superiority is the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same. Achieving information superiority is key to winning future battles.

Part of the solution to achieving and maintaining information superiority is a robust grid of interoperable networks covering the globe, providing the warfighter with access to high-speed voice, video, data, imagery, telemetry, sensory, and multimedia information. The instrument to transport this information to the warfighter is the Global Information Grid - Air Force concept.

The GIG-AF concept establishes the architecture to transport to the warfighter, the information they need, when and where they need it while ensuring the protection of both the information and its means of transport. The GIG-AF links fixed AF bases to our airborne and deployed forces.

The GIG-AF supports air warfare, space operations, air mobility, special operations, combat support, information operations, command and control, intelligence, and humanitarian relief operations worldwide. The GIG-AF is divided into four infrastructure components:

*Outside the Gate* encompasses all the components required for information transport between all Air Force bases, deployed sites, federal agencies, sister services, and allied forces. These components comprise the wide area network. The WAN provides the warfighter connectivity to all domains of electronic information transfer, both military and non-military, CONUS and OCONUS.

Warfighters and weapons systems (airborne and deployed) are linked across the globe using both terrestrial and space-based communications systems. This linkage comes from using DOD common user information networks, via a site's service delivery point into the WAN. This service delivery point is the dividing point between outside-the-gate and inside-the-gate infrastructures.

*Inside the Gate* comprises all components required for information transport across a site's metropolitan

area network. The MAN is the connection or backbone network between the service delivery point and all essential community of interests at a site. This backbone provides the connectivity that links the members of a COI, warfighters, weapon systems, commanders and other users, across a base or a deployed site.

This connectivity consists of optical fiber cable, wireless communications, and core applications services and network management systems. The site's network system extends the communications capabilities down to the local area network or last 400 feet infrastructure established within a site's facilities.

*Last 400 Feet* covers the LAN components required for transporting information within a COI's network system. This network links users, warfighters and commanders, to information and core services that allow them to support mission operations.

This linkage is the cabling, both copper and fiber optic, wireless connectivity, floor/wall connections, LAN hardware and software.

The components usually are contained within a building but depending on the COI site (deployed), the LAN can span multiple facilities. The network

provides the connections where a user can access the LAN through information appliances.

*Information Appliances* are the end devices of the communication path provided by the LAN, MAN, and WAN. These devices are used to enter and extract information and provide the last portion of end-to-end connectivity to the warfighter. Information appliances encompass all computer-processing workstations, shared devices and peripherals, office automation software, and end-user telecommunications systems.

Information appliances are used in the in-garrison office, airborne, deployed, and remote environments. Information appliances provide high-speed processing, massive electronic storage, multimedia hardware and software, end-user voice, video, and data telecommunications devices, personal wireless communication systems, office automation software, and message services in an open system and common operating environment.

The GIG-AF is the high capacity, protected, global communications infrastructure that transports the information the warfighters need, when they want it, where they need it. The next time you send voice, video, data, multimedia or sensor information to a warfighter anywhere in the world in a secure and timely fashion, it is due to the implementation of the GIG-AF.



# Assessing the hacker threat

By Capt. John Kissack and Anna Gorka  
82nd Computer Systems Squadron, Langley AFB, Va.

Each day the Air Force increases its arsenal to improve our network's fortress wall. We are doing everything necessary to protect our information systems by keeping the hacker out, right? Some experts in the computer security community would disagree.

To minimize this threat, we must first understand the community we are dealing with. Hackers, or more accurately crackers, are idealistic and often rationalize their actions with "Robin Hood-like" thinking. They are the underdog fighting a force in the only way they think is possible. The hacker community does not see the damage done to real people or to the nation that gives them the freedom to form their subculture.

So, how do we defend against this enemy? Consider these points:

- ✓ Assume the threat to your network is there and act upon it. Be aware, be security conscious.
- ✓ The information technology world is changing rapidly and constantly. Keep up with current trends and informed of the hacker activity.
- ✓ Know your team members. Create an environment where every person is an important part of the effort. Hold workers to the responsibility of keeping the system secure and sanction computer security abusers. Foster an atmosphere of a team whereby input is welcomed from every team member.
- ✓ Make certain that your computer security personnel are given adequate training and the authority to do their job. Make your security team a strong, full-time entity. Commander support of computer security is essential.
- ✓ Know thy enemy. Be aware of what is happening in your organization and in the information assurance arena. Learn from other's mistakes and share your own for the good of the security community.

Cultivating a sense of ownership, pride, and purpose in our organizations is essential in this age of downsizing. Make sure your team understands the importance of their individual role in protecting government information systems.

**Scenario:** It's your turn to pull watch. Although there has been a lot of recent activity in your sector, it's been classified as non-hostile—looks like it's going to be another uneventful shift. Suddenly, you realize you're under a full-scale attack—your enemy has breached your security measures undetected, went straight to the weaknesses in your defenses, and has exploited them. Before you can react, the enemy quickly realizes they have been detected and disappears, tak-

ing with them their spoils, leaving a path of destruction in their wake.

The sentry in this scenario is your computer system administrator; the perimeter he guards, your computer system's network connection; the enemy, the hacker community. Although the military community is concerned with this malicious activity, every system with connectivity to the internet, military or commercial, is a potential target for a hacker attack.

Following are key observations of the hacker community, based on both personal experiences in the ACC Network Operations and Security Center and research of hacker practices. This is by no means an exhaustive list, it merely tries to identify significant threats a hacker poses to the legitimate computing world.

► Observation 1: The enemy is organized. Not only does the hacker have proven computer system attack methods and procedures, he freely shares with the hacker community his "lessons learned". Hackers have demonstrated their ability to coordinate sophisticated attacks, concealing real hacker attacks with innocuous network traffic or other diversionary attacks.

► Observation 2: The enemy practices "social engineering". This is probably the most insidious of the hacker practices. Until recently, many computer security policies instructed that users only accept e-mails and their associated attachments from "trusted sources". Social engineering attacks such as the Melissa and Worm virus made computer security experts re-visit the definition of a trusted source. In both of these instances, the viruses spread by sending virus copies to the infected user's trusted sources, such as personal e-mail address lists. And although these attacks made the computer community a little less naïve, this attack will undoubtedly surface again, only this time from a different angle.

► Observation 3: The enemy has plenty of resources. It only takes a quick browse of the internet to see the pervasiveness of hacker-oriented web sites. Readily available are hacker tips, methods, and software tools that automate hacker attacks, such as mapping your network topology (probes) or exploiting known system vulnerabilities.

► Observation 4: The enemy is relentlessly testing your defenses. Probing activity has been on the increase for the past year, and is continuing its upward trend. This electronic test for services can determine what kind of system you have, such as UNIX, Windows NT, etc. Once the system type is known, the real attack using known exploits can commence.

Continue the vigilance, protect our Air Force network weapon system.

## DEFENDING AGAINST THE ENEMY

*Assume threat to your network is there and act upon it.*

*Keep up with current trends and informed of the hacker activity.*

*Know your team members.*

*Make sure your computer security personnel are given adequate training/authority to do their job.*

*Know thy enemy.*

# Staying up with latest software version

By Master Sgt. Cindy Crowe

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

It never fails. Just when you think you've got a software program down pat and know what you're doing, the next version appears. So, for all of those CAW operators, who think they have CAW Version 3.1 down, watch out because CAW Version 4.2.1 will be here before you know it.

The transition from version 3.1 to the CAW Version 4.2.1 will be starting in the April/May timeframe, but it will take approximately 18 to 24 months or longer to upgrade all CAWs.

The Air Force will receive about 50 copies of the software this fiscal year. Since training is NOT Air Force funded, major commands have identified priority sites to receive the software based on the fact that the unit or major command has the funding to send two individuals to training. So, if you're one of those units who didn't have the TDY money this fiscal year for the training, plan ahead for FY01. You're going to need it.

The training class for the CAW Version 4.2.1 will be about eight to 10 days. Individuals will be trained on all CAW positions (Certification Authority/System Administrator/ Information Systems Security Officer). Two individuals per base must be trained, and the CAW positions must be identified to NSA before the new CA cards will be sent to the base.

Currently, for version 3.1 there are two separate classes, one to train the Certification Authority/System Security Officer Organizational Registration Authority and one for the SA/ISSO. With version 4.2.1 it will be one class to teach the CA/SA/ISSO. Once trained on

the CAW Version 4.2.1, if the CA deploys and needs to become the SA/ISSO at the deployed location, no additional training is required. The individual can be deployed without being sent back to training before the deployment.

Training en route before going overseas is encouraged rather than having to send the individual back from the overseas location. This should be worked through the functional managers to ensure the individuals are identified and trained en route.

Currently, units are identifying inputs to Air Education and Training Command for the CAW Version 3.1 classes. Since one classroom will be upgraded to CAW Version 4.2.1, it is desirable that, except for emergencies (i.e., unexpected PCS, retirement, etc.), whenever possible, new students would be trained on the CAW 4.2.1 version software. CAW Version 3.1 classes would only be run when needed.

Remember the nasty rumors about requiring an upgrade to all issued FORTEZZA cards again? Well, it's true. All cards must be upgraded from version 1 certificates to the version 3 certificates. Version 3 certificates will have more precedence capabilities and security categories for sending and receiving messages. These capabilities will be used when DMS version 3.0 is available. We suggest you write a transition plan to upgrade the FORTEZZA cards. Determine which user's mission requires the additional capabilities and upgrade these cards first. We suggest you schedule the rest of the users so the workcenter is not overworked at any one time.

Remember, version 1 will be compatible for a period of time (during the transition) after release of DMS Version 3.0.

## *Policies for Participating in chat forums*

By Senior Master Sgt.

**Chris Hedge**

*Air Force Communications Agency*

Recent trends illustrate an increase in Air Force personnel participating in chat forums from base networks. AFI 33-129, Transmission of Information via the Internet, generally prohibits official use of these forums without prior approval from public affairs channels due to the increased operations security vulnerabilities.

Additionally, dial-up access to Internet service providers, such as America On Line, CompuServe, or

others, is prohibited for users with Internet access through base and deployed networks, except when an organizational subscription is established for official business. Participating in chat forums from home can also create operations security vulnerabilities.

Policies against communicating with unauthorized personnel apply to Internet communications regardless of whether you're on or off duty. These chat arenas provide personnel the opportunity to converse electronically to a worldwide audience; however, military and government employees must refrain from dis-

cussing sensitive work-related issues in these **open** forums. Such discussions could result in potential unauthorized disclosure of sensitive information.

For example, anyone monitoring the Internet may construe conversations from government employees as official statements or government positions on specific topics.

Using the Internet creates various security and OPSEC problems and supervisors must ensure policies are enforced and everyone understands the risks associated with using the Internet from home or work.

# AMC's Network Operations and Security Center is state trooper of the information highway

By Capt. Jason Buster  
and Keith Gilbreath

*Network Operations and Security Center*

**SCOTT AIR FORCE BASE, ILL.** – In today's environment, we are dependent on fast, accurate information systems and networks to meet our mission. In short, our systems and networks have become "centers of gravity." Our adversaries are keenly aware of this and constantly look for ways to compromise our systems. The frightening aspect of their activities is that it usually only takes one weakness in one system for an intruder to wreak havoc throughout a network. As the quote goes, "A risk imposed by one, is a risk assumed by all." This makes information assurance one of the Air Force's top priorities.

Air Mobility Command takes the IA challenge very seriously and is at the forefront of Air Force efforts to send and defend information. If you're a bad guy on the information highway, we're gonna pull you over! The Network Operations and Security Center is AMC's "state trooper" (command center) for the IA mission. As such, it exercises command and control over AMC's entire network enterprise using several related, but distinct avenues of attack. The NOSC ensures that: 1) networks are available, 2) networks maintain integrity, 3) transmissions are authentic, and 4) transmissions are protected.

First, the NOSC ensures that networks, systems, and applications are **available** to AMC bases, en routes, and deployed locations (the state trooper clearing accidents so other vehicles can get through). When the NOSC is aware of an outage, they log it into a trouble-ticketing system. Depending on the nature of the outage, they can assist the customer from our command and control, intransit visibility, or office information system help desks or through commandwide support contracts. The AMC NOSC help desks successfully resolve an amazing 70 percent of all calls at Level One (the industry standard is 40 percent).

To help us in really tight spots, we've enlisted the help of Microsoft Premier Support. AMC is the first

command to employ this top flight contractual support to ensure our dependence on Microsoft Windows products is not a hindrance to network availability. At the NOSC, we not only use the trouble ticket reporting system to track problem resolution, but we share our knowledge base with all base network control centers.

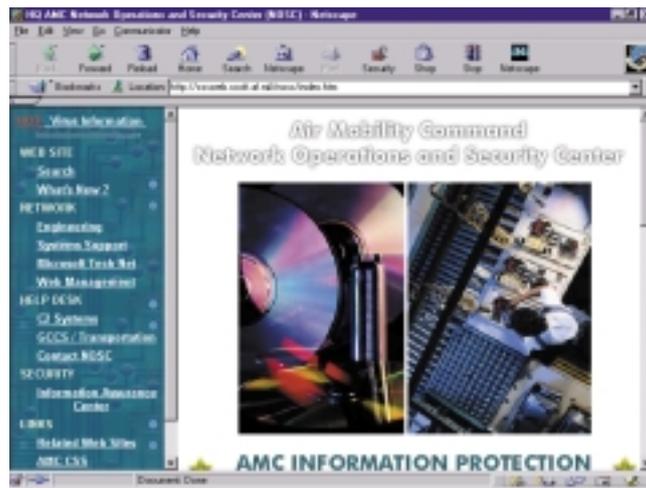
Second, the NOSC continually assesses the **integrity** of information systems and networks within the command. Integrity is defined here as a seamless network devoid of vulnerabilities that could be exploited by an adversary (state trooper reports holes in the

interstate's limited access fence). The NOSC uses online survey, auditing, and hacking tools to identify vulnerabilities in our C2 systems. The NOSC also requires the NCCs to perform similar procedures on their base-level systems.

Here again, AMC is on the leading edge in network integrity. The NOSC uses an in-house developed tool called MetTraks to track each NCC's progress toward ensuring network integrity.

MetTraks also allows the NOSC to track compliance with Air Force Computer Emergency Response Team advisories as well as certification and accreditation status. Also, the AMC NOSC is one of the first to purchase a software tool that has the capability to push software vulnerability patches down to the desktop. NOSC personnel also visit NCCs to help perform vulnerability assessments and train users on the best security practices. Finally, we evaluate new hacking exploits, security, and auditing tools to assist NCC customers in maintaining the highest security posture possible.

Next, the NOSC analyzes AMC networks and systems traffic on both a near real-time and off-line basis. The information is collected by the Automated Security Incident Measurement sensors located at each base. The NOSC reviews this information to determine the **authenticity** of each connection (the trooper pulls you over and asks to see your license). If they determine



See TROOPERS Page 40

*intercom*

39

## TROOPERS From Page 39

the traffic is unauthorized, they notify various Air Force organizations to ensure the Computer Network Defense systems (routers, firewalls, gateways and host level access controls) are readied against the threat. The NOSC's 24-hour presence ensures the base CND mission is continuously monitored and protected.

Finally, **protection of information during transmission** is also of key concern to the AMC NOSC (state trooper intercepts travelers who are driving recklessly, without seatbelts or in an unauthorized vehicle; keeps authorized travelers safe; ensures they reach their destination). We are involved in evaluating Public Key Infrastructure technologies to enhance the confidentiality of our mission data as it traverses less secure networks.

An example of a Public Key Infrastructure-like technology is the Secure Socket Layer protocol for web-based communication. The Secure Socket Layer service allows clients to interrogate the identity of web servers. Once the identity of the web site is confirmed, a secure session is set up between client and host to prevent eavesdropping or hijacking. Several AMC systems are using this technology already. As an IA frontrunner, the NOSC is also a member of the Air Force Public Key Infrastructure steering group to determine ways to implement more of this technology for other types of network-based interactions (e.g. financial transactions, official communications, etc.).

While the NOSC is at the forefront of the AMC IA mission, all of us must be aware of network vulnerabilities and our responsibilities as network users. We're keeping the reckless drivers off the information highway; but, you've gotta buckle up!

# Compromising information -- for the sake of convenience

By **Herbert P. Cooley**  
*Wing Computer Security Manager*  
*Luke AFB, Ariz.*

Convenient ways to communicate come in many different forms. For example, there are speaker phones, computer microphones, Net meetings, e-mail, cellular telephones, wireless telephones, the Internet, wireless keyboards, Web TV, satellite communications, using file servers that exchange information in a common folder, and video teleconferencing. The technological ability to converse with anyone, at a moment's notice, relies heavily upon performance and productivity as the driving force, without taking into consideration the aspects of protecting this exchange of information while it is being transmitted.

To further this notion of productivity and efficiency, a second notion has emerged. This notion is that every newly manufactured technological device ensures anyone can perform at the highest level of production if only they use it. The consequences of applying these notions fuels the idea that the latest device will achieve the best results. While these devices, such as speaker phones, wireless telephones, cellular phones, or Net meetings, may be efficient, if the information being conveyed is compromised while using the device, it undermines another notion of protecting that information. This is the flaw that has emerged from this technological revolution.

Due to the technological revolution in telecommunications, it has become more complicated for an individual to understand all of the vulnerabilities associated with new devices. This is because the lines of

emissions, computer, communications, and operations security disciplines have been convoluted. If an individual does not understand the vulnerabilities of the device they will be using, the consequences could be devastating. Individuals are being exploited on a daily basis. For example, individual's credit reports are being altered; credit card numbers are being stolen; critical information being found on command Web home pages is used to enable terrorist acts, and criminals are using the Internet for unscrupulous activity. As our adversaries begin to level the "playing field" by using the

Due to the technological revolution in telecommunications, it has become more complicated for an individual to understand all of the vulnerabilities associated with new devices.

same type of technology against the United States, it is imperative for everyone to understand the importance of safeguarding information.

To prevent information from being compromised, an individual must have an understanding of what type of forum the data or information is being exchanged or processed and the vulnerabilities associated with the forum. By ensuring proper safeguards to protect the information are being conveyed, the data can proceed with integrity and non-repudiation to the warfighter on the battlefield. It is not an option to waive the oath to safeguard national security information for the sake of convenience.

Though societal pressures will continue to influence our decisions, we must take a moment to plan to ensure information will be protected before exchanging information via new technology. These precautions will ensure we will not undermine the Air Force's technological advantage to out-manuever our next adversary and will lighten the strain on the equipment that processes the required data to conduct air operations.

# Ceremony marks opening of GCSS office

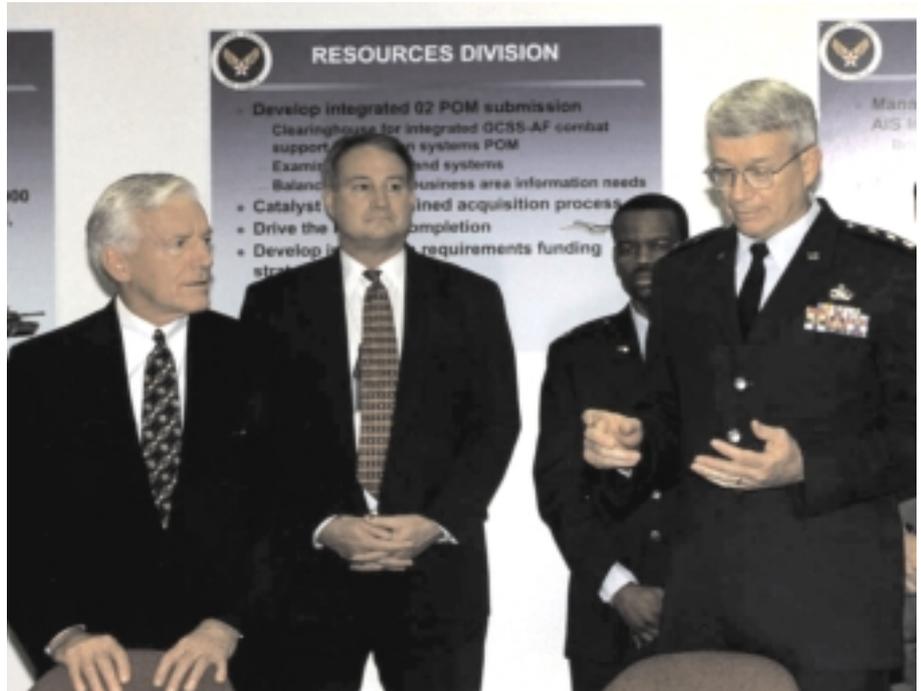
By Capt. John Jarvis  
*Air Force Communications and  
Information Center  
Pentagon*

The Global Combat Support System – Air Force Requirements Integration Directorate had its directorate opening ceremony Nov. 1.

The primary objective of GCSS-AF is to combine mission-essential, non-command-and-control, functional AIS requirements to the Air Force, Air Force Reserve, and Air National Guard, with combat support Automated Information Systems requirements allocated to support the Joint Chief’s GCSS strategy for achieving Focused Logistics.

The Air Force has developed the strategic vision called *Global Engagement: A Vision for the 21st Century Air Force*. This vision includes six core competencies that apply directly to the Joint Vision concepts. Four of these Air Force core competencies — Precision Engagement, Rapid Global Mobility, Information Superiority, and Agile Combat Support — relate directly to accomplishing Focused Logistics and require GCSS-AF implementation.

GCSS-AF started in the late 1980s under the program name, Base Level Systems Modernization.



**Dr. Lawrence Delaney, Air Force Chief Information Officer, (left), Steve Farish, MITRE, and Lt. Col. Freddie McSears, Aerospace Command and Control, Intelligence, Surveillance, and Reconnaissance Center, listen as Lt. Gen. William J. Donahue, Air Force/SC, explains the importance of GCSS-AF during the GCSS-AF Directorate ceremony.**

BLSM was then an umbrella program to support the incremental modernization of the Standard Base Level Systems environment for the Air Force, Air Force Reserve, and Air National Guard. BLSM had three major goals:

- (1) Integrate the base-level combat support systems to enhance decision support for the wing commander.
- (2) Migrate base-level systems to an open, nonproprietary architecture to reduce costs.
- (3) Incorporate functional business process improvements to improve overall effectiveness and efficiency.

These three goals are still valid, but the Air Force vision has continued to evolve. The primary goals of GCSS-AF now include supporting the joint warfighter by providing

ACS to implement the Expeditionary Aerospace Force.

The primary mission area initially supported by GCSS-AF was information systems/defense communications systems. Collateral mission areas supported by GCSS-AF were base operations, contingency base operations, mobility, support and base communications, strategic information systems, and service-support activities.

The GCSS-AF concept has evolved over the years and now includes hundreds of AIS spread across 13 functional areas: logistics, civil engineering, services, contracting, medical, personnel, operations, manpower, systems support, information management, security police, environmental support, and comptroller. These AIS provide information to support effective use of DOD and allied forces.

# Don't miss out on available training, information opportunities

By Don Fizer

*CICP Professional Development Administrator*

If you haven't visited the Communications and Information Career Program web site lately, you're missing out on information that can enhance your Air Force civilian career. Set time aside now and periodically visit: [www.af.randolph.af.mil/cp/cicp](http://www.af.randolph.af.mil/cp/cicp).

Under the "Training" heading you can click on any hot button for immediate information or access to pages containing information regarding various training opportunities and general guidance.

The following information is available:

- 1) 2000 Program Guide for Management Development Center classes
- 2) National Defense University classes leading to Chief Information Officer Certification
- 3) Basic and Advanced Communications-Information Officer's Training
- 4) Aerospace Basic Course
- 5) Squadron Officer's School
- 6) A-76 training

- 7) Acquisition classes leading to certification
- 8) Calendar of interactive television classes available through the Government Education and Training Network
- 9) FY99 (and soon FY00) on-site course schedule
- 10) Tuition assistance
- 11) Education with Industry and Industrial Development Education in Acquisition
- 12) Available classes, titles with codes, for use in the Career Enhancement Plan preparation.

You can also find out what training classes are listed in your records by visiting the CICP web site. Click on the "Record Review" tab and follow the instructions. If your training records are incomplete, contact your local Civilian Personnel Flight.

Please allow at least a month for your training to be listed into the system before taking any action. Also don't forget to ask your Civilian Personnel Flight to place "do not drop" indicators besides important training classes.

Contact the CICP professional development office at DSN 665-3691, for training information.

## Air Force balances security with access to e-mail

WASHINGTON (AFPN) — As the Air Force continues efforts to shore up its computer network defenses, officials remain committed to providing deployed troops access to the Internet for morale purposes. Even as commanders remain committed to providing deployed troops access to morale e-mail, they must also consider security in the information realm.

To help reduce this security risk, the Air Force is taking steps to block access on its networks to tools such as commercial e-mail services and Internet chat links, "which provide an unacceptable risk to our networks by offering easy avenues of attack," said Chief Master Sgt. Ray Kennedy, business systems analyst, Air Force Directorate of Communications and Information Support

Systems Branch.

"The World Wide Web and e-mail are technologies that have become deeply intertwined with Air Force mission processes." However, Kennedy stressed, actions being taken will not eliminate troops' access to morale e-mail.

"Our networks are under attack everyday by hackers and malicious code writers, and we expect increased activity by those who would use the Y2K rollover as an opportunity to conduct mischief," the chief noted.

"Our people's quality of life is of paramount importance to every commander and these technologies play a vital role in meeting their needs," Kennedy said.

"Commanders are encouraged to provide morale e-mail services via

.mil accounts as much as possible, within the limits of their particular security and network capacity."

One tool the chief cited is "GI Mail" developed by Air Mobility Command, which meets the service's security policy.

"GI Mail is currently undergoing upgrades that will enable even wider access by users outside the .mil domain, yet still meet stringent security requirements," Kennedy said.

"The Air Force strongly supports morale e-mail and other safe uses of the Internet, but these must be carefully balanced with mission security requirements.

He said, "We will continue working hard to provide the best morale services we can without putting our networks at risk."

*Daily postal operations are a warm-up for the holiday season*



*Photo by Master Sgt. Val Gempis*

**YOKOTA AIR BASE, Japan (AFPN) -- Tech. Sgt. Christopher Pease, a postal augmentee from 118th Communications Flight, Tennessee Air National Guard, assists personnel from Detachment 2, Pacific Air Forces Air Postal Squadron, with sorting and distributing to the postal service centers at Yokota, Camp Zama and Misawa Air Base. The postal professionals of Det. 2 work hard to ensure quality service to their customers through economical transportation and highly efficient operations. The detachment processes more than 30 million pounds of mail a year.**



*Photo by Eddie Edge*

**From left, Staff Sgt. Eric Boyd, 938th Engineering Installation Squadron, and Senior Airman Sean Sikora, 738th EIS, align a localizer distribution unit.**

## EIS team enhances Tinker runway

**TINKER AIR FORCE BASE, Okla.** — A project is nearing completion to install an Instrument Landing System which provides final approach guidance to aircraft in all weather conditions, a laser cloud ceiling detection system, and an airfield visibility system. As a result of these runway enhancements, Tinker AFB will have an instrument approach to a runway where none previously existed. This provides for a safer flight environment for Tinker and the surrounding area and will provide a fully operational runway during the renovation of another runway.

The runway improvement project began in September 1998 when the 72nd Communications Squadron Meteorological Navigational Maintenance work center completed a self-help installation of a Localizer for the runway. The Localizer provides center of runway information to aircraft on final ap-

proach and included the installation of 14 antennas, aligning all equipment, and passing a rigorous flight inspection by the FAA.

In August, a team from the 938th Engineering and Installation Squadron arrived from McClellan AFB, Calif., and Keesler AFB, Miss., to complete the rest of the equipment installation.

The 938th EIS team constructed a 50-foot tower for three antennas, a 14-antenna array, and aligned two separate systems. The weather equipment installation consisted of the construction of four towers and platforms ranging from six to 17 feet, mounted and aligned six transmitters and receivers, and mounted various indicators in both the Air Traffic Control tower and the Base Weather Station.

The cost of the ILS/Weather project was about \$1.2 million and became operational at the end of 1999. *(Courtesy of the 72nd CS)*

**"We're going to celebrate our victories  
and pave the way  
for continued progress in our mission  
to provide Information Assurance  
across our Air Force."**

*Lt. Gen. William J. Donahue  
Director of Communications and Information*