

# intercom

Journal of the Air Force C4 community ☆ October 2004



Warfighters depend on

## **INFORMATION ASSURANCE**

- ▶ The three pillars of IA ▶ Defending the networks
- ▶ Confidence in emission security ▶ Viruses & hackers

# intercom



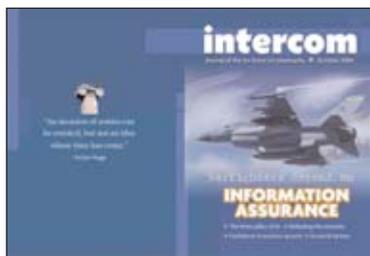
**4** From the **Top**: Aerospace dominance and the pillars of Information Assurance  
Col. Gregory Brundidge



**12** Information Assurance and the deployed warfighter  
Mr. Jim Taratino



**20** Advanced Extreme High Frequency system  
AF Space Command



Cover illustration by Marine Lance Cpl. Sean Murphey. Design by Master Sgt. Karen Pettitt.

- 4 **From the Top**: Aerospace dominance and the pillars of Information Assurance  
*Col. Gregory Brundidge*
- 8 Uncle Sam wants you to defend our networks  
*Mr. Donald Poole*
- 9 The changing faces of viruses and hackers  
*Staff Sgt. Nicholas Martychenko*
- 10 What you need to know about USB storage devices  
*2nd Lt. David Williams*
- 11 Security for wireless systems  
*Master Sgt. Dave Hammack*
- System certification process  
*Lt. Col. Bruce Harmon*
- 12 IA for the deployed warfighter  
*Mr. Jim Taratino*
- 14 Team provides emissions security  
*Capt. Adam Lenfestey*
- 20 Advanced Extreme High Frequency system  
*Air Force Space Command*
- 21 SCOPE Network becomes SCOPE EDGE  
*Maj. John Hoeft*
- 24 Operations and Exercises require multi-level security methods  
*1st Lt. James Bressendorff*
- 25 **Time Machine**: Reflections  
*Mr. Gerald Sonnenberg*
- 26 **Civilian Focus**: SCOPE champion; **News Briefs**: DMS, patch notification, ROBE, IDEA facility, tactics, awards, ratings, customer service, NOSC guards, postal warriors.
- 30 **Techno Gizmo**: Public Key Enabling  
*AFCA WFP*



**22** Biometrics: A logical choice for logical access?  
*Ms. Michelle Dugan*

THE JOURNAL OF THE AIR FORCE C4 COMMUNITY

**Gen. John P. Jumper**  
Air Force Chief of Staff

**Lt. Gen. Tom Hobbins**  
Deputy Chief of Staff for Warfighting Integration

**Lt. Gen. Ronald E. Keys**  
Deputy Chief of Staff for Air and Space Operations

**Lt. Gen. Donald J. Wetekam**  
Deputy Chief of Staff for Installations and Logistics

**Maj. Gen. Charles E. Croom Jr.**  
Director of C4ISR Infrastructure  
DCS for Warfighting Integration

**Brig. Gen. (sel) Ronnie Hawkins**  
Director of Communications Operations

EDITORIAL STAFF

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

**Lori Manske**  
AFCA Chief of Public Affairs

**Master Sgt. Karen Pettitt**  
Managing Editor

**Tech. Sgt. Jim Verchio**  
Editor

This funded Air Force magazine, published by Helmer Printing, N. 6402 790th St., Beldenville, Wis., 54003, is an authorized publication for members of the U.S. military services. Contents of the intercom are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or the Department of the Air Force. Editorial content is edited, prepared and provided by the public affairs office of AFCA.

<http://usaf.smartforce.com>

Submitting to the intercom

Stories should be in Microsoft Word format and should be no longer than 600 words. Photographs should be at least 5x7 in size and 300 dpi. Submit stories via e-mail to [intercom@scott.af.mil](mailto:intercom@scott.af.mil).

Subscription requests

E-mail all mailing requests or address changes to [intercom@scott.af.mil](mailto:intercom@scott.af.mil).

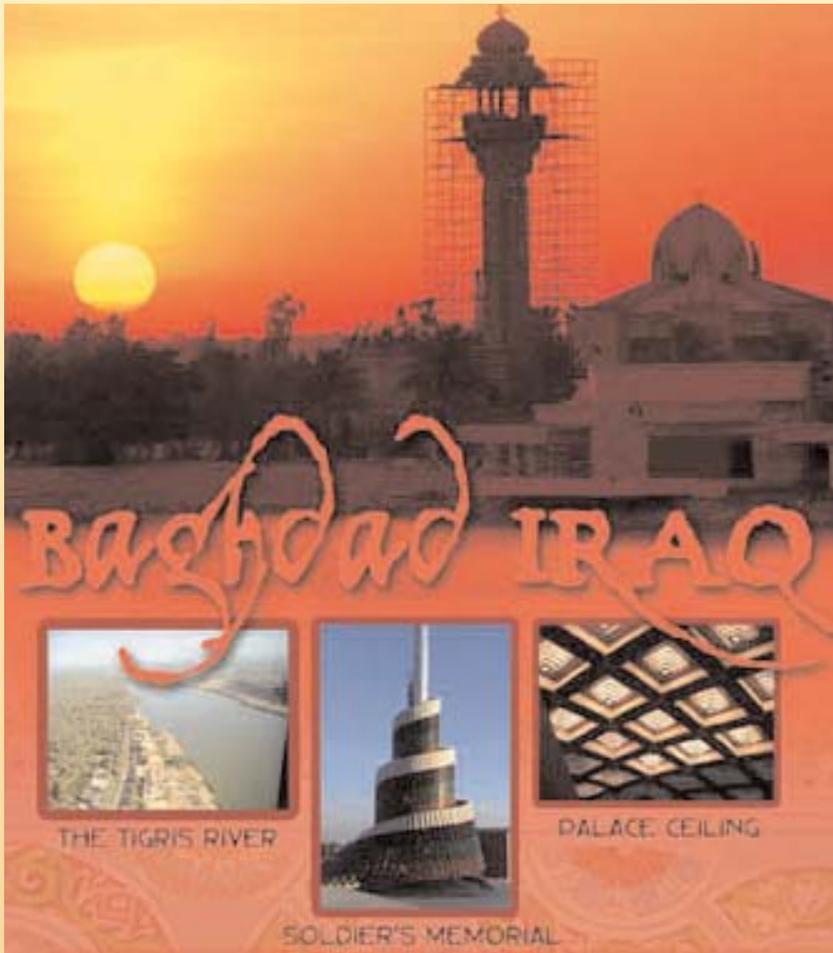
Comments to the staff

Comments, and letters to the editor, may be e-mailed or sent via the postal service to AFCA/PA, intercom, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222.

AWARDS FOR 2003

- Most Improved Magazine & Honorable Mention
- Clarion Award \* Women in Communications**  
Award of excellence - Internal Magazine
- NAGC Blue Pencil Competition**  
Best Online Newspaper
- Air Force Media Contest**  
Best Designed Publication
- DoD's MILGRAPH Competition**

## From the editorial desk



**By Master Sgt. Karen Petitt**  
Intercom Managing Editor

While there are many communicators serving throughout the world, there are none more dear to my heart than those serving in Baghdad, Iraq. They're there working in beastly 115-degree heat, dodging mortars and scanning the roads for improvised bombs. They're dealing with customers who want more bandwidth, more phone lines ... more of everything. Things there are physically difficult and emotionally draining, yet every comm person I came across, whether Air Force, Navy or Army, had positive attitudes. They understood their mission and, even though the mission became frustrating at times, they could always be counted on to make things happen. Getting laptops to work, installing additional phone lines, setting up internet cafes, maintaining servers, keeping commanders linked to their units throughout Iraq and setting up better ways to provide satellite communications take on extra meaning in Baghdad. Nothing's easy there. Nothing! So the things we think should take an hour may take four hours or may need a whole different approach. These comm folks allowed our coalition partners and the Interim Iraqi Government to function well. A special thanks to them for their commitment, hard work and outstanding support!

**JAG**  
in a **Box**

**Fritz Mihelcic**  
AFCA Deputy  
Chief Counsel



### Get legal advice

**I've attended one of your briefings and based on what you said, I may be doing something illegal that my supervisor asked me to do. What should I do?**

**A** Because Information Technology issues are often complex, your best response is to inform your supervisor that you were briefed in this area and suggest calling the experts [AFCA/JA] for our assessment.

We recognize many IT issues are high-visibility and enjoy senior-level interest, but this is all the more reason to ensure there are no legal roadblocks that could stall the mission.

A key element of the "Integrity First" core value is ensuring what you do complies with the law. You should never forgo seeking legal advice because of "command pressures." Bringing us into the loop when you think you have a problem will pay dividends for you later. We usually provide answers to questions while we're talking to you, meaning you won't have to wait days or weeks to get an answer. This up front legal advice could avoid disastrous consequences for you, your boss, and your project down the road. Play it safe and call the lawyers—we're here for you!

**Send in your question to:**

**AFCA-JA@scott.af.mil**  
or call DSN: 779-6060

# AEROSPACE



From  
the **Top**

**By Col. Gregory Brundidge**

PACAF Director of Communications and Information

To meet the demands of today's net-centric ops environment or battlespace, we must adapt a much broader construct for Information Assurance. Aerospace dominance, time-sensitive targeting, predictive battlespace awareness, and effects-based operations are now today's essential operational realities. Looking forward, we must further evolve these realities to achieve total battlespace awareness supporting real-time decision-making. At the center of all of these major operational muscle movements is "the net" - the aggregate of all network connectivity (terrestrial, airborne, and space), capabilities and processes. In this net-centric environment, information assurance is not simply ensuring that information is protected, accurate and delivered on time, but it is also ensuring that all the components involved in making that happen are postured, prepared, and ready to do so. To define IA requirements for the "net-centric" environment, we must widen the aperture and include more than the "-icities, -ilities, and -ations" normally associated with information assurance. For the big "IA" we must consider three pillars of technology, processes and people.

# DOMINANCE & THE PILLARS OF

# INFORMATION ASSURANCE



## TECHNOLOGY

Relevant technical capabilities and mission-driven innovation

As industry continues to improve Information Technology capabilities to process, exchange, transfer and store more information, faster and better, we must demand the parallel development of information protection capabilities. The ability to achieve authentication, integrity, confidentiality, non-repudiation, and availability—the traditional elements of information assurance or what we call small “ia”—relies heavily on technologies that are on par with advancing information processing, networking, and storage capabilities. So, it’s not only important for us to be competent with today’s “ia” technologies, but we must always have an eye on the “ia” technologies for tomorrow. **Encryption, intrusion detection, firewall, and authentication tools for our networks must evolve and grow with other network capabilities.** This is especially important as more of these technologies are designed into network components vice the stand alone, add-on boxes. By staying in touch with those who perform network operations and deliver the full spectrum of network services, those who acquire these capabilities can ensure they deliver timely, usable, and relevant technologies for tomorrow’s “ia” demands. Failure to do this will lead to “late-to-need” technology advances, and result in unacceptable vulnerabilities and flaws in the net. **Equally as important as keeping “ia” technologies current, is the need to standardize on vendor solutions or, as a minimum, provide specifications for vendors to meet when providing hardware or software components for the net-centric environment.** This is an essential step to eliminating hard-to-manage, service disrupting variability in our networks and corresponding self-inflicted training and budget challenges in our control centers. We don’t acquire other weapon systems this way and neither do we expect our aircrews, and air, space, and missile operators to have to train for unmanaged variability in the systems they operate.

## PROCESSES

CONOPS & TTPs

To achieve the desired product of a fully capable net-centric ops environment, the process for delivering the product is as important as the product itself.

Remember that the net-centric ops environment is the aggregate of all network connectivity, capabilities/services, and processes from the physical layer connections and protocols to net-enabled operational processes and applications. **To effectively command and control this environment there must be well defined CONOPS, policies, and procedures for governance, operation, and sustainment.**

Because NETOPS in the net-centric environment is a young operational discipline, we are in the process of developing many of these governing and guiding documents today.

The process component of big “IA” is critical because it enables optimized use of available technological capabilities. It does no good to have



superior information technology in our control centers if we don't have the processes in place that enable us to leverage its power and transform it into meaningful and relevant operational capability for the warfighter.

**How often have we raced to field the latest hardware or software network tool or application only to complete fielding and find that we didn't evolve our ops concepts and procedures so that our net technicians and users could leverage its full capability?**

To develop, implement, and sustain viable net-centric processes, it's imperative that we apply strong ops rigor and discipline to current NETOPS policy and Tactics, Techniques and Procedures and adopt a capability-driven model for developing and implementing new network tools.

The advent of a centralized standardization and evaluation program, such as SCOPE EDGE, is a critical first step.

It should form the foundation of a broader stan/eval construct that will assess all critical processes delivering the net-centric environment, to include network management, network administration, network defense and associated NOSC and NCC crew operations.

We will know we've achieved success when the TTP, checklists, bold print, and technical orders that govern these processes are in place.

Today, we routinely bring new capability as technology makes it available and then develop the required CONOPS driven processes and procedures after the fact, if at all.

Instead, **we must use a capability-driven model that brings new network capability as ops requirements dictate and adjusts CONOPS and associated processes and procedures prior to fielding.**

Ideally, we also train our technicians in advance, so we can transparently implement new capabilities without disrupting current NETOPS.

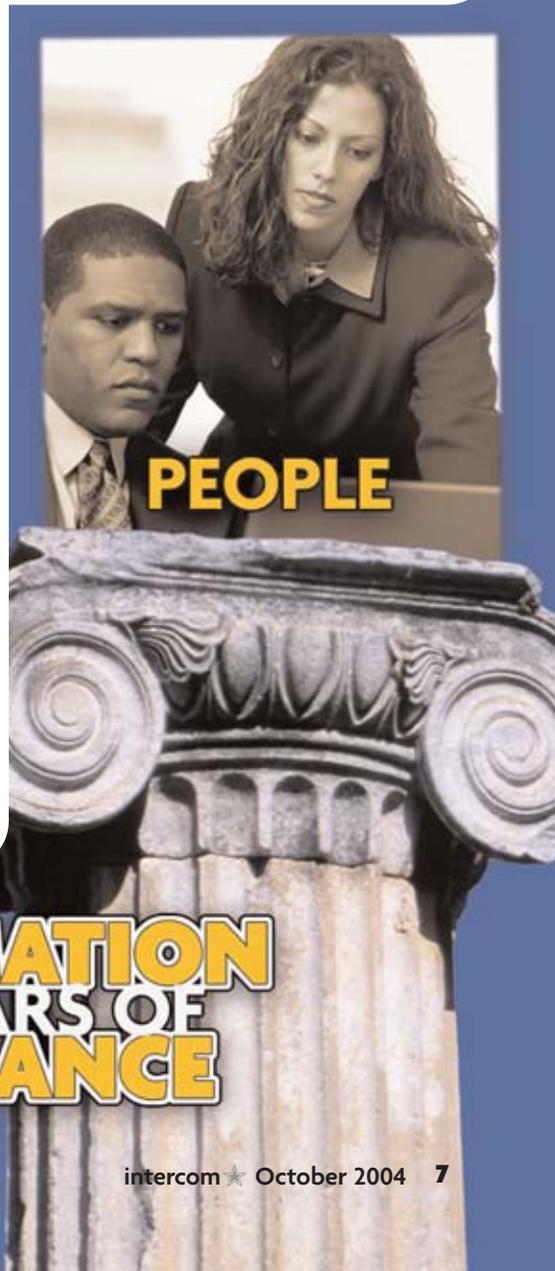
## PEOPLE

### Indoctrination, Training and Development

Drive-by fieldings, poor or no ops rigor and discipline, constantly changing configuration baselines, training turmoil and deficiencies, and non-standard hardware and software suites are all part of the environment in which we expect our network professionals to succeed. **The mindset of the net professional must be transformed from the world of data processing and specialized computing and messaging centers in which many of our mid-and senior-level technicians grew up.** In the net-centric environment, the essential mindset is one that understands the interdependencies of the net and fully appreciates the importance of standards in our technologies and processes. The transformed net professional realizes that a network risk or vulnerability assumed by one is assumed by all. To complete the necessary mindset transformation, we start with training processes that span the development cycle for the technician. From tech school to 7-level training, the program must be focused on building "interchangeable" net technicians. In addition to standardized training, we should endeavor to "push the envelope" wherever possible and take net warrior training to the next level. In industry, credibility comes from not only being able to deliver capabilities upon demand, but also from the level of certification one brings to the table. We should work toward getting our people

mission-driven certifications recognized by the industry but focused on highlighting higher degrees of mission qualification. **Certifications such as "Certified Information Systems Security Professional," "Project Management Professional" and "Security A+" could equate to "specialist," "senior specialist" and "master specialist" ratings.** These ratings would mark the difference between those who dabble in our field and those whom we would consider to be experts. This produces a "win-win" situation for our military, our civilian counterparts, and for the individual. Additionally, it raises the bar for improving net-centric operations across all dimensions of the mission area.

As we standardize hardware and software on our nets, and the TTP we use to employ them, we pave the way for completing the necessary mindset transformation.



## Uncle Sam WANTS YOU to defend



# OUR NETWORKS!

**By Mr. Donald Poole**  
ACC IT Assessment Branch

**LANGLEY AFB, Va.** — In November 2003, Brig. Gen. (Sel) Ronnie Hawkins, Air Force Director of Communications Operations, mandated annual information assurance training by all Air Force personnel: military, civilian and contractors.

To ensure everyone is trained to the same standard, the AF Information Assurance Awareness 2004 course was developed and launched at the Smartforce computer-based training Web site. This course describes the importance of the role to which users participate in the defense of our information and information systems, law, policies, terminologies, methods of exploitation and what authorization of activities are authorized/unauthorized. Network Centric Warfare,

Common Access Card, Public Key Infrastructure, malicious code, hoaxes and spam are discussed in detail, explaining both benefits and results of proper/improper network operation. Through annual recertification, unintentional threats will be reduced and our warfighters will remain able to fight.

Network security protects and prevents loss of critical communications. Interruptions or denial of network services affect our war

fighting ability. Defense-in-depth is applied to the outer perimeter of Air Force networks with firewalls, anti-virus scanners and blocking devices. However, the primary threat is not from intentional or malicious activity, but from unintentional human error.

Our proactive enthusiasm in defending our nation from enemies both foreign and domestic is taken personally when we complete the Information Assurance Awareness CBT module. We strengthen the interior network perimeter and fulfill our Air Force's Federal Information Security Management Act reporting when we understand the value of Information Assurance. Taking the course, living the lessons learned, and sharing those principles with our fellow Airmen will enable each of us to protect and defend the United States.

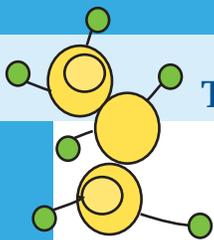
### How do we do that?

Complete the USAF Information Assurance Awareness Course  
<http://usaf.smartforce.com>

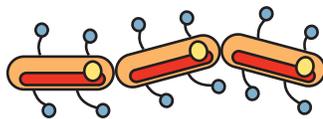
Live the lessons learned

Teach the principles to our fellow Airmen





The worst virus that can get onto our network is the one not discovered.



# The changing faces of viruses & hackers



By Staff Sgt. Nicholas Martychenko  
28th Communications Squadron

ELLSWORTH AFB, S.D. —There were hackers and viruses back when the Internet was but a fledgling collection of Tandys, Macs, prehistoric IBMs, and text-based bulletin board sites. They were just there in different forms and using different methods.

Back then there were no firewall programs, proxy servers or antivirus software. All you had between you and them was your password and logon. And, if anyone got your SYSAD password, God help you.

Hackers could get unlimited capabilities over your BBS and anything you had on it. At that time, hacking was just a matter of patience and knowing your enemy. Hacking was viewed as a harmless prank on a friend and could be done using names or birthdates. It seems simple, right? Indeed, it was all too simple.

The face of the virus has changed as well. **It used to be that viruses could not be self-activating. They had to be activated from the computer itself after being uploaded to memory.** The viruses were not complex; they were incredibly simple, yet destructive. A simple command to format the hard drive imbedded in the program, sometimes elaborately hidden in a text-based game that the user would download to their computer and then play. When they completed the “game,” they were rewarded with the one thing no computer user ever wants to see: the involuntary formatting of their primary hard drive.

While this may all seem harmless and rudimentary now, it was but a foreshadowing of what was to come. We now

live in a time when many of our most valuable assets exist only in the space between two computer chips. Many facets of our lives have been boiled down to a string of 1s and 0s. It’s unsettling to think that by changing just one of those digits, our lives could be forever altered, rarely to the good.

Computer security, information security and network protection are practices that need to be ingrained in everyone as second nature. **Much like keeping your checkbook in a secure place, passwords must be protected. Memorization is the only true protection we have left.**

Viruses have evolved quickly in the past two decades. No longer are they passive programs, waiting for user activation. They invade, they replicate, they destroy and they do it with an efficiency that we can hardly counter.

Antivirus software is one of the tools that we have that allow us to stem the tide of destruction and chaos that viruses represent.

But much like a tetanus inoculation, it only works if you are still conscientious and aware of what is going on. The shot helps, but stepping on a rusty nail only gains you the need for another booster. Viruses are like that, so keep your antivirus software up to date with the most recent signatures and scan your computer monthly.

It’s paramount that all network users, whether they are logged on to a DoD system or their own home computers, maintain a level of awareness that will allow for systemic degradation recognition and reporting.

11010110

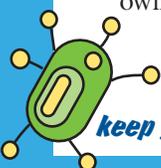
Know your enemy, know their weaknesses, and learn how to exploit them.

A hacker’s weakness is tight security and educated end-users.

A virus’ weakness is an up-to-date virus signature and software that recognizes viral patterns of destruction.



110101



*keep your antivirus software up to date with the most recent signatures and scan your computer monthly*

What you need to know about

## USB Storage Devices

protecting your information

**By Master Sgt. Josh Walker**

AFCIA Information Systems Security Policy

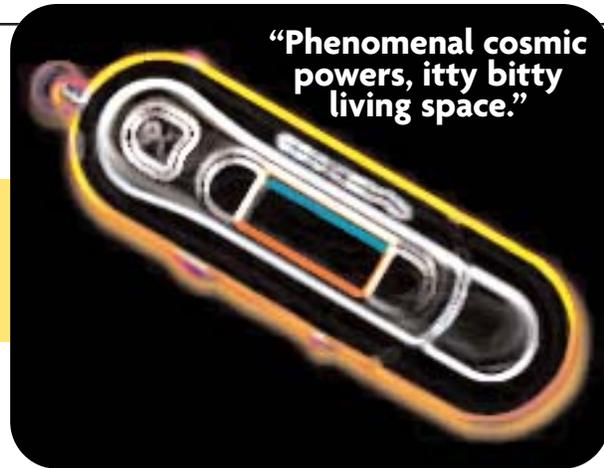
**SCOTT AFB, Ill.** —As with any new technology, there are risks associated with usage, and USB storage devices are no exception.

**USB storage devices can easily introduce viruses into a computer network.** Anti-virus filters and firewalls are installed to protect and defend today's computer networks against viruses. However, using USB storage devices bypasses those security mechanisms because they plug directly into a computer potentially allowing a new virus or worm to spread across the entire network. Because USB storage capabilities are so massive, there's also the potential of bringing in other dangerous and unauthorized software including shareware, freeware and spyware.

**The second major risk in using USB storage devices is data loss or theft.** Any unattended USB storage device or any unlocked computer with a USB port becomes a rich source of sensitive information. The thief could be anyone, making the insider threat that much more dangerous. A person may simply lose the device since it's so small. If someone finds it, they may return it but what if it fell into the wrong hands? If someone simply borrows your USB storage device and returns it to you, will it now have a virus?

**Using USB storage devices in a classified environment presents other risks.** Because most of these devices don't have write protection mechanisms, placing a USB storage device into a classified computer makes it classified at the same level as the system. **There's currently no approved utility to sanitize flash memory.** Once classified, you must use the storage device only in classified environments or, when no longer needed,

Portable Universal Serial Bus storage devices are, essentially, flash memory drives (sometimes called thumb or pen drives) capable of storing 1Mb to 5GB of information. Compatible with just about any computer with a USB port, files can transfer at a rate of 1Mb per second without a separate power supply or battery. It can be reused more than one million times and preserved for more than 10 years.

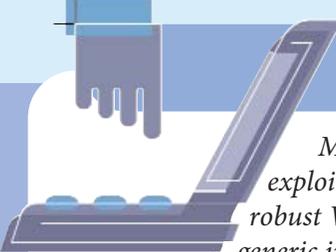


destroy it. Many organizations do not wish to accept the risks of using USB storage devices in classified environments and have prohibited their use.

Becoming aware of the risks with using these devices is a great beginning to safeguarding information. Air Force Instructions does not specifically mention USB storage devices, but they are a form of portable/removable media and therefore subject to all Air Force policies regarding media. This includes, but is not limited to AFI 33-202, Network and Computer Security, and Air Force Systems Security Instruction 5020, Remanence Security.

**To prevent someone from downloading information to a USB storage device, ensure the system has a password-protected screen saver enabled and remove common access cards from readers before leaving the computer unattended. Ensure the use of antivirus software, keep it up-to-date and use it. Scan all removable media, including USB storage devices, for viruses before each use.** Some USB storage devices come with additional security features like password protection, encryption and biometrics.

Before buying one, find out if your organization has a policy on approved USB storage devices. Ensure the media is marked and labeled IAW AFI 31-401, Information Security Program Management. Marking and labeling will help control media during loss and prevent inadvertent use of unclassified USB storage devices in classified computers. USB storage devices are portable, handy and have incredible storage capabilities. They also have a few security challenges. Unfortunately, there is no single magic spell to counter the risks presented by them. Awareness of the risks is the best method of protecting information or, in other words, keep the genie in the bottle and the power in the palm of your hand.



# Security for wireless systems

Modern hackers are choosing the newest and most vulnerable information system to exploit—the Wireless Local Area Network. Fortunately, it's relatively easy to secure even robust WLANs from those that would cause the most harm. The following steps are fairly generic in terms to wireless networking and will apply to almost all WLANs.

▶ **Activate the built-in wireless encryption.** Wired Equivalent Privacy was the first attempt at providing some measure of security in wireless networks. Because several free-ware hacking tools are available to “crack” WEP keys, WEP should not be used alone to protect WLANs. Future standards for wireless encryption include Wi-Fi Protected Access (WPA - an enhanced version of WEP) that uses key caching and AES encryption. Currently, DOD and Air Force WLAN security policies provide guidance on using encryption to secure WLANs.

▶ **Update the WLAN interface card and access point software.** Security-conscious manufacturers provide patches to software that fix security issues. Hardware often sits on shelves for weeks and months, and one or more patches may have been created during that time.

▶ **Change the access point default password and WLAN network name, or Service Set Identifier-SSID.** A common step when setting up a WLAN is to change the default passwords/SSIDs on access points. System administrators spend so much time in the setup that they often forget to go back and change these critical settings once the net-

work is running. Some will move back to factory defaults (no security at all) when they are reset.

▶ **Install all WLAN access points in securable areas.** Don't leave APs unsecured where they can be easily accessed, or even switched by a hacker with their own AP so it will accept access from anyone. If the AP is not used during specific times of the day, disable it by unplugging it. If there are several APs in the WLAN, installing “Power-over-Ethernet” equipment from a central location will make this administrative task easier to manage.

▶ **For users accessing the WLAN, installing Virtual Private Network technology** on their clients will secure their access to sensitive information and applications. IP Security Protocol VPN software will provide the necessary levels of encryption and access control required by DOD and AF security policy, and give the user peace of mind when they are transferring information across the WLAN. If the wireless internet service provider allows a VPN connection, this is a good idea for home wireless networking as well.

— Master Sgt. Dave Hammack AF Network Security Program Manager

## System certification process

The computer system you're using most likely went through four independent reviews before it was allowed to operate on the Air Force enterprise network. This certification team consists of program managers, system engineers, user representatives, Designated Approving Authority representatives, information system security officers, and others as needed, to develop and document in a system security authorization agreement the system's security architecture and policies. By understanding the process, you will be more careful in how you operate and take care of your system.

— Lt. Col. Bruce Harmon AETC Cyber Security Branch

### CERTIFICATION TEAM

The certification team performs comprehensive testing and evaluations to ensure agreed upon security measures are used. After rigorous review and testing, the Certifier certifies to the DAA that the system meets network security requirements, and if a particular requirement cannot be fully met, recommends risk mitigation procedures.

### AIR FORCE COMMUNICATIONS AGENCY

AFCA validates the certification team's findings and recommendations through an independent assessment of the system's security features and architecture. This assessment is documented in the issuance of a “Certificate of Networkiness.”

### MAJCOM REVIEW

Although the primary emphasis is on sustainment issues such as fielding schedules, network bandwidth usage, and allied support, the system's security is again reviewed to ensure the system meets MAJCOM-unique needs. The MAJCOM review is documented in a “Certificate to Operate.”

### BASE-LEVEL ASSESSMENT

The base Information Systems Security Manager, in conjunction with the program management office and the base network control center ensure the system is installed and operated from the agreement developed by the certification team.



# IA for the deployed

Basic tools of boundary protection, misuse detection and internal system controls allow comm to flow

By Mr. Jim Taratino  
Air Combat Command

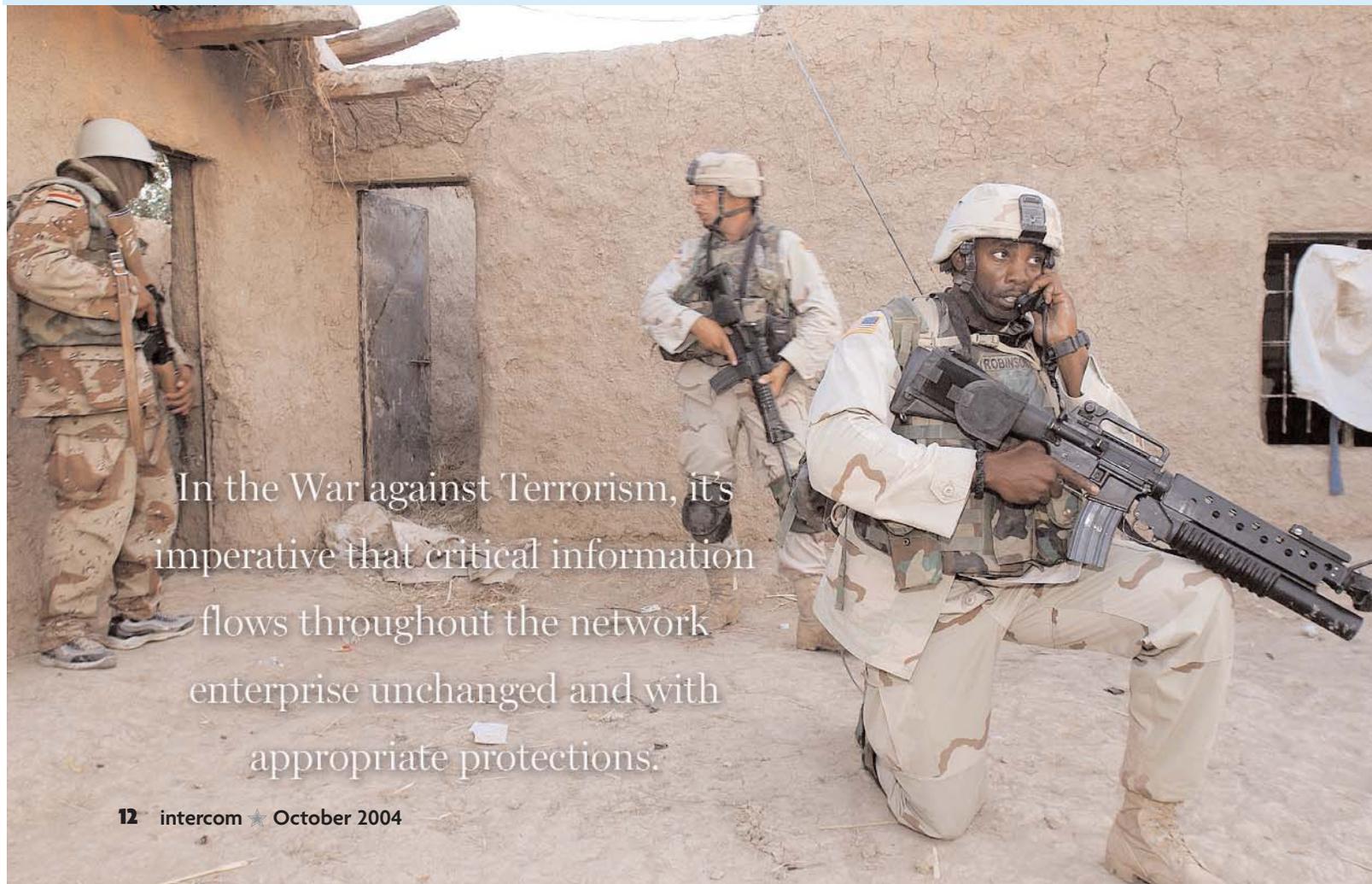
LANGLEY AFB, Va. — During Desert Storm, the deployed communications infrastructure provided the warfighter with secure and non-secure voice services and minimal data services. Ten years later, during Operation Iraqi Freedom, the deployed communications infrastructure provided the warfighter with a host of services, including information assurance tools that protected critical data throughout the spectrum of the war.

IA is the corner stone for

data transfer that ensures the data is delivered intact, protected, and unchanged.

In the deployed environment, base-level IA tools are provided by the Theater Deployable Communications program.

These tools consist of boundary protection, intrusion and misuse detection, and internal system controls, all of which are modeled after the Combat Information Transport System architecture used at the fixed bases. Maximizing the use of tools common to the CITS baseline not only ensures interoperability and improves integration, but also eases the training burden, enforces standards, and streamlines operations.



In the War against Terrorism, it's imperative that critical information flows throughout the network enterprise unchanged and with appropriate protections.

# warfighter

## BOUNDARY PROTECTION

The main boundary protection features protect the network perimeter by providing a means to control the information that crosses the network boundary.

The primary equipment used to enforce this protection includes an external router and the firewall. A Web Proxy Server and a Split Domain Name System Server also support the boundary protection role.

**As the first line of defense, the external router protects the screened subnet as well as the interior network from the external Internet.** It performs this function primarily through IP level packet filtering based on source and destination address and protocol.

In doing so, it resists IP spoofing attacks. In addition, the external router “screens” the firewall from direct attack. This is important since routers typically offer fewer services than host machines, such as firewalls, and hence are less vulnerable to a direct attack.

**The Sidewinder firewall furnishes the bulk of the boundary protection services.** The TDC design uses a “dual dual-homed proxy” firewall, which has two network connections — one to the internal network and one to the exter-

nal network. By not allowing direct connections between the internal and external networks, the firewall protects internal users from the rest of the Internet.

## INTRUSION AND MISUSE DETECTION

At the network perimeter, intrusion detection functionality is provided at the firewall.

Because the architecture contains a consolidated access point, the firewall is able to provide intrusion/misuse detection for all non-web base traffic.

**The intrusion/misuse function performed by the firewall is to detect and report unauthorized base network access and to attempt identification of potential attackers.**

The host-based solution is Symantec Host IDS software. The HIDS software is hosted on the Network Management Server running Microsoft Windows 2003.

## INTERNAL SYSTEM CONTROLS

The internal system controls are capable of assessing security issues such as proper password length, server configurations, access control rules, and user account administration. It also assists in the enforcement of network and security policies. The TDC

program provides two software packages to provide internal system controls: Symantec Enterprise Security Manager and Internet Security Scanner.

ESM is hosted on the Network Management Server while agent software is installed on all network control servers (except for the external primary DNS server) and most network servers.

**It checks for vulnerabilities and potential security holes in account integrity, login parameters, password strength, file systems and directories, network and server settings, system queues, and startup scripts.**

ISS is a protection mechanism offering integrity and security management. It is hosted on the “security” workstation to “learn” network vulnerabilities by performing a series of tests for well-known vulnerabilities.

Password Policy is enforced by Windows 2003.





# Team provides confidence in EMSEC emission security



courtesy photo

Barry Booth tests desktop computers for the E-4B National Airborne Operations Center. (Left) Senior leaders rely on the 346th Test Squadron's Specialized Test Flight to keep their comm secure.



**By Capt. Adam Lenfestey**

Air Intelligence Agency

**LACKLAND AFB, Texas** — What the Air Force calls Emission Security, or EMSEC, is known in DoD terminology as TEMPEST, and is a cornerstone of Information Assurance. TEMPEST standards must be checked to ensure pieces of equipment processing information at different classification levels are physically separated by predetermined distances to prevent them from electromagnetically interfering with each other.

In some cases it's either not possible to enforce a set of rules about separation such as in the tight spaces inside aircraft, or the information being processed is so sensitive that decision-makers need to know the "ground truth" about their system. That's where the Air Force's only EMSEC instrumented test team comes in. **Any aircraft, facility, or device in the Air Force that processes classified information is a potential test subject for the 346th Test Squadron's Specialized Test Flight.** They've tested virtually every type of aircraft in the inventory, from venerable airframes like the B-52, C-130 and KC-135 to our most advanced weapon systems such as the B-2 and F/A-22. **Their expertise has even been used by other government agencies, such as NASA, which needed to ensure the security of space shuttle communications.**

In some cases there may be only one secure radio. In others, such as the E-4B National Airborne Operations Center, there are several hundred interconnected units supporting multiple strategic-level missions. These systems often include components operating at many different levels of classification and sensitivity, from unclassified Internet, satellite telephone, and air traffic control channels to top secret military communications, including some of the most sensitive information in the U.S. gov-

ernment. In addition to aircraft, the team tests Air Force facilities for unintentional radiation of classified data, including locations in the continental U.S. and around the globe. **From sunny garden spots such as the Air Force Research Lab's Maui Space Surveillance Site to cloudy RAF Lakenheath, England; from frozen Elmendorf AFB, Alaska, to baking-hot Saudi Arabia, they've been there.**

The team also operates and maintains anechoic chambers where they test emissions from laptop computers, video teleconferencing switches, PDAs and other electronic devices in an electromagnetically shielded facility. In this laboratory environment, the device being tested is isolated from any outside interference, which allows testers to take more precise measurements.

**EMSEC testing needs to be performed nearly any time the configuration of a communications system is changed, so the team routinely tests many of the same assets year after year as older analog radios and switches are upgraded to newer digital versions.** The test team has to understand the components in a system—how they work and how they interact with each other—in order to plan their testing appropriately, and understanding ever-changing technology is a major challenge as the systems become increasingly complex.

EMSEC testers have traditionally had to understand electronics, radio signal propagation, and electromagnetic coupling. Now they've added digital signaling protocols, spread-spectrum techniques and other advanced technologies to their repertoire. And as the systems being tested become more advanced, the instrumentation used to test them also grows more complex. The team has recently upgraded its old analog receivers in favor of newer digital models and has acquired some other new gear. And, no matter the challenge, the 346th's efforts provide confidence to senior leaders who must have secure comm.

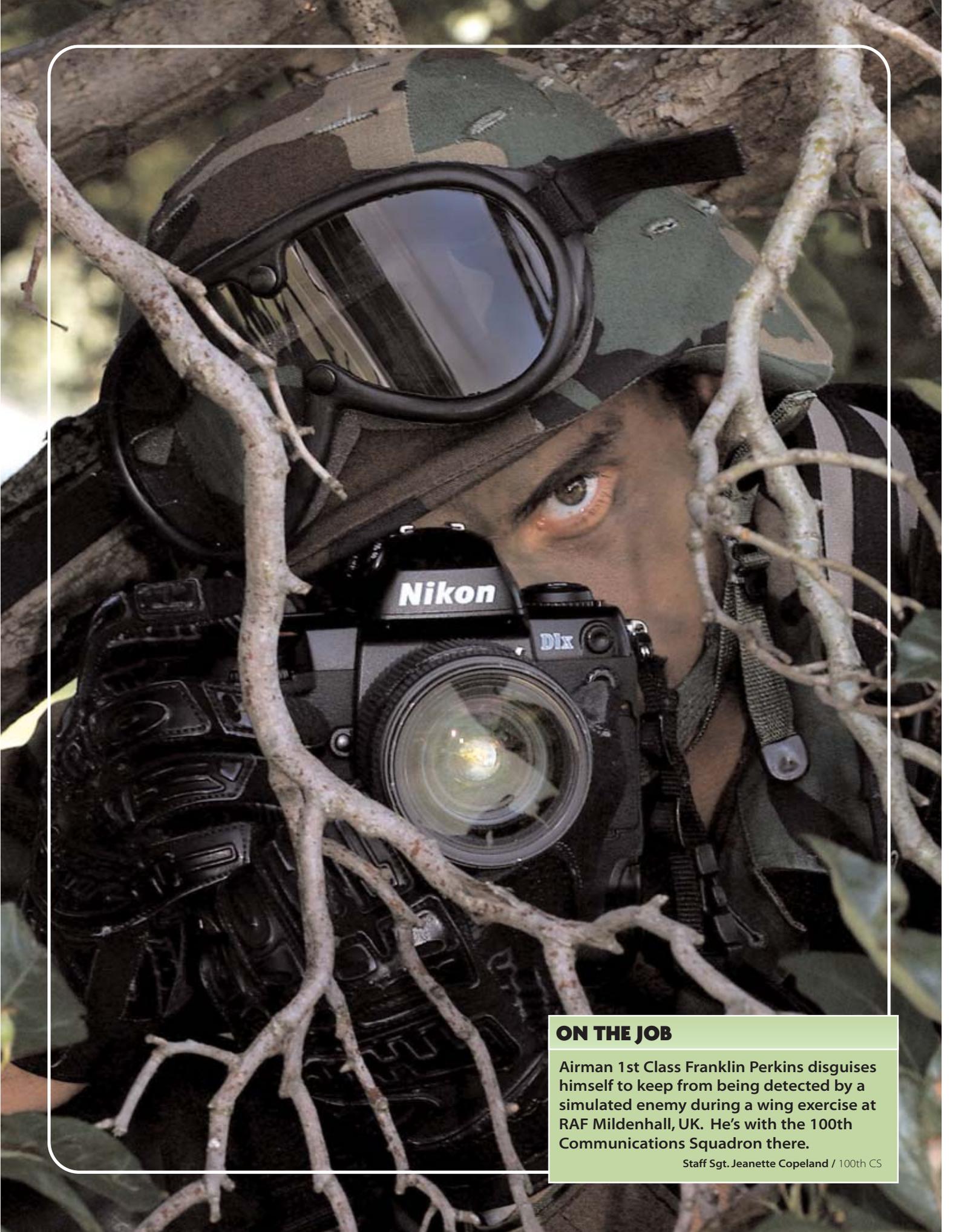
## BOSNIAN CELEBRATION

The nationally renowned "Old Bridge" or "Stari Most" of Mostar, Bosnia, was officially opened July 23 with fireworks, ceremonies and a gathering of high profile dignitaries. NATO Stabilization Force supported the event with communications and aerial support.

Tech. Sgt. Cecilio Ricardo / 1st CTCS







**ON THE JOB**

Airman 1st Class Franklin Perkins disguises himself to keep from being detected by a simulated enemy during a wing exercise at RAF Mildenhall, UK. He's with the 100th Communications Squadron there.

Staff Sgt. Jeanette Copeland / 100th CS

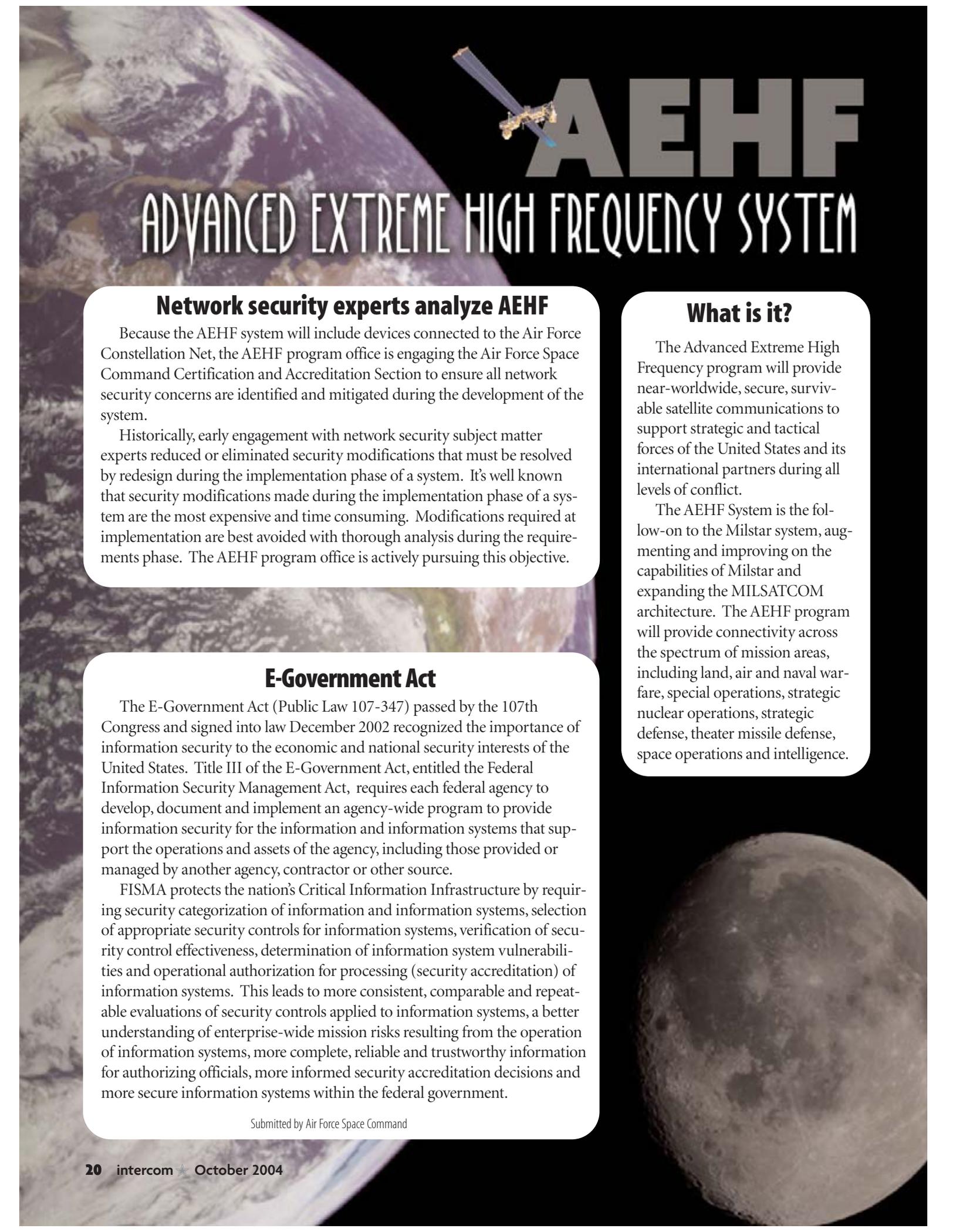


## COUNTER TERRORISM TRAINING

Air Force members who belong to Tactical Air Control Party teams coordinate air assets for training members of the Iraqi Counter Terrorism Force. This group is getting ready for fast rope training, just one of the many skills being taught jointly by Air Force special operations members and Army Special Forces teams in Baghdad, Iraq.

*Army Spec. Joshua Joyce / MNC-I PAO*





# AEHF

## ADVANCED EXTREME HIGH FREQUENCY SYSTEM

### **Network security experts analyze AEHF**

Because the AEHF system will include devices connected to the Air Force Constellation Net, the AEHF program office is engaging the Air Force Space Command Certification and Accreditation Section to ensure all network security concerns are identified and mitigated during the development of the system.

Historically, early engagement with network security subject matter experts reduced or eliminated security modifications that must be resolved by redesign during the implementation phase of a system. It's well known that security modifications made during the implementation phase of a system are the most expensive and time consuming. Modifications required at implementation are best avoided with thorough analysis during the requirements phase. The AEHF program office is actively pursuing this objective.

### **E-Government Act**

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act, requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source.

FISMA protects the nation's Critical Information Infrastructure by requiring security categorization of information and information systems, selection of appropriate security controls for information systems, verification of security control effectiveness, determination of information system vulnerabilities and operational authorization for processing (security accreditation) of information systems. This leads to more consistent, comparable and repeatable evaluations of security controls applied to information systems, a better understanding of enterprise-wide mission risks resulting from the operation of information systems, more complete, reliable and trustworthy information for authorizing officials, more informed security accreditation decisions and more secure information systems within the federal government.

Submitted by Air Force Space Command

### **What is it?**

The Advanced Extreme High Frequency program will provide near-worldwide, secure, survivable satellite communications to support strategic and tactical forces of the United States and its international partners during all levels of conflict.

The AEHF System is the follow-on to the Milstar system, augmenting and improving on the capabilities of Milstar and expanding the MILSATCOM architecture. The AEHF program will provide connectivity across the spectrum of mission areas, including land, air and naval warfare, special operations, strategic nuclear operations, strategic defense, theater missile defense, space operations and intelligence.

# SCOPE Network becomes SCOPE EDGE

By Maj. John Hoeft

Chief Network Optimization Branch

**SCOTT AFB, Ill.** — The Air Force Communications Agency recently transitioned from SCOPE Network teams that focused on optimizing and securing base networks to what they now call SCOPE EDGE teams. EDGE stands for Enterprise, Design, Guidance and Evaluation.

SCOPE Network had focused on optimizing and securing the existing base network equipment to obtain the peak performance from it and train Network Control Center personnel to maintain that equipment. Now that NCCs have established procedures for maintaining the network weapons system, it's time to change.

**SCOPE EDGE will now be looking at the network as an enterprise instead of as a collection of 130 bases.** SCOPE EDGE personnel reviewed Air Force Instructions and technical order guidance and created an authoritative checklist of items which

can be measured and are not contradicted by other guidance. Contradictory guidance is being deconflicted. This checklist will be used to evaluate base networks for compliance with architectures and standards.

**SCOPE EDGE will perform Base Optimization visits for two reasons.** First, to help bases which are struggling to overcome problems due to aging equipment or with an influx of new equipment or personnel. For optimizations **SCOPE EDGE will use Network Health Criteria based on the Network Maturity Model with the grading scale of Optimized, Controlled, Documented and Chaotic.**

Second, to maintain SCOPE EDGE personnel base network optimization skills so they can perform Strike Force contingency operation missions. Strike Force contingency operations will send experienced SCOPE EDGE members to augment base NCC personnel or separately to provide network engineering expertise where needed. To accomplish all of this within the resources allot-

ted, SCOPE EDGE will present its forces differently than SCOPE Network. Each MAJCOM is assigned a Team Chief who will coordinate all actions with the MAJCOM SC or A6 staff. **Together the MAJCOM and the Team Chief establish a schedule for compliance, NOSC optimization and base optimization visits.** Instead of performing all actions on site as SCOPE Network did, SCOPE EDGE will perform many actions remotely.

For compliance visits, teams will scan the network remotely and assess it for compliance as much as possible. Then a base visit will assess items which could not be validated remotely.

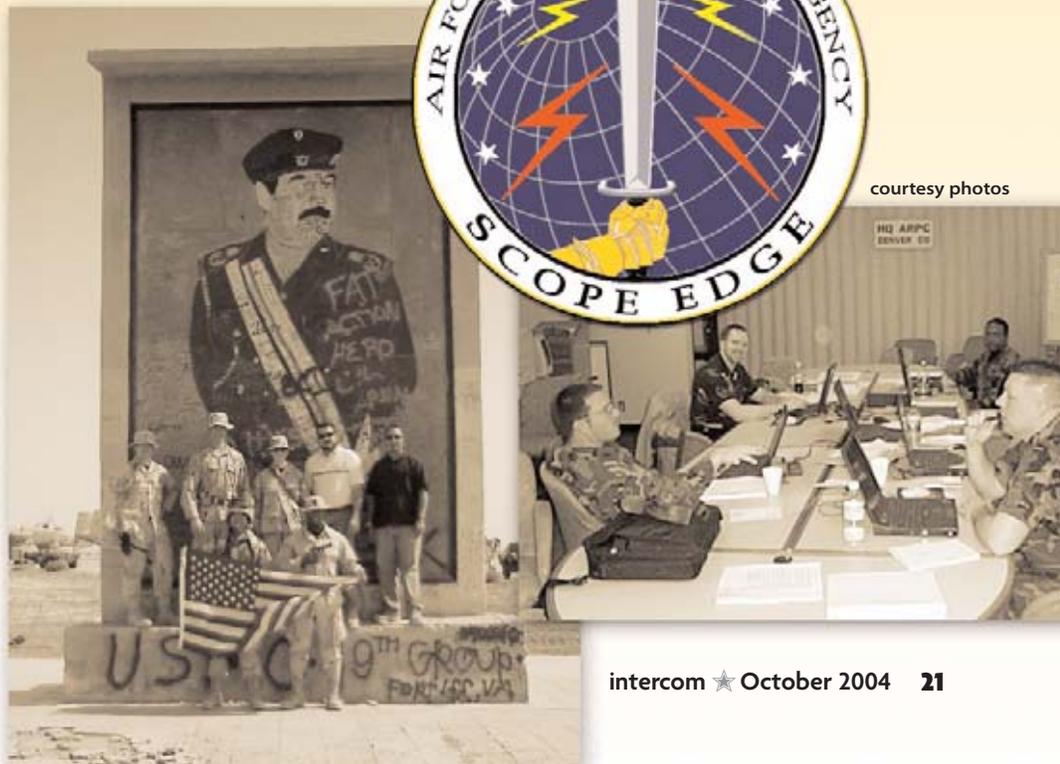
For optimization visits, a similar scan will be performed to obtain the data required to analyze the network and determine what actions are required for optimization. When the analysis is complete, a team will visit to optimize and secure the network in collaboration with

base NCC members.

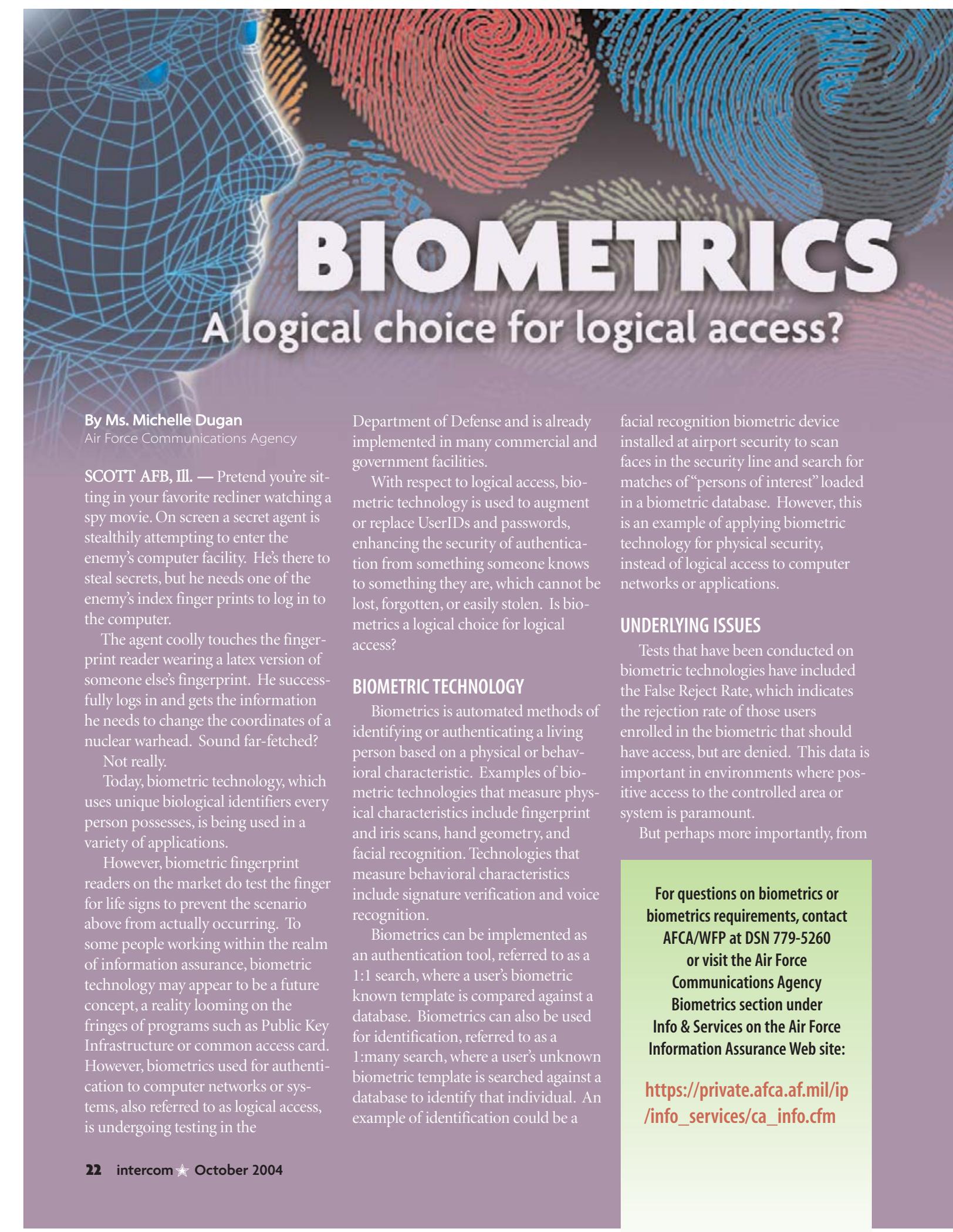
## 4 mission areas

- ▶▶ Evaluate base networks for compliance with architectures and standards;
- ▶▶ Optimize NOSC networks to mature their operational readiness and security of their operations;
- ▶▶ Provide Strike Forces to perform contingency operations and provide targeted network engineering expertise to establish C2 nodes;
- ▶▶ Optimize some base networks that still need assistance and maintain Strike Force skills to optimize base networks.

[private.afca.af.mil/scopeedge](http://private.afca.af.mil/scopeedge)



courtesy photos



# BIOMETRICS

## A logical choice for logical access?

By Ms. Michelle Dugan

Air Force Communications Agency

**SCOTT AFB, Ill.** — Pretend you're sitting in your favorite recliner watching a spy movie. On screen a secret agent is stealthily attempting to enter the enemy's computer facility. He's there to steal secrets, but he needs one of the enemy's index finger prints to log in to the computer.

The agent coolly touches the fingerprint reader wearing a latex version of someone else's fingerprint. He successfully logs in and gets the information he needs to change the coordinates of a nuclear warhead. Sound far-fetched?

Not really.

Today, biometric technology, which uses unique biological identifiers every person possesses, is being used in a variety of applications.

However, biometric fingerprint readers on the market do test the finger for life signs to prevent the scenario above from actually occurring. To some people working within the realm of information assurance, biometric technology may appear to be a future concept, a reality looming on the fringes of programs such as Public Key Infrastructure or common access card. However, biometrics used for authentication to computer networks or systems, also referred to as logical access, is undergoing testing in the

Department of Defense and is already implemented in many commercial and government facilities.

With respect to logical access, biometric technology is used to augment or replace UserIDs and passwords, enhancing the security of authentication from something someone knows to something they are, which cannot be lost, forgotten, or easily stolen. Is biometrics a logical choice for logical access?

### BIOMETRIC TECHNOLOGY

Biometrics is automated methods of identifying or authenticating a living person based on a physical or behavioral characteristic. Examples of biometric technologies that measure physical characteristics include fingerprint and iris scans, hand geometry, and facial recognition. Technologies that measure behavioral characteristics include signature verification and voice recognition.

Biometrics can be implemented as an authentication tool, referred to as a 1:1 search, where a user's biometric known template is compared against a database. Biometrics can also be used for identification, referred to as a 1:many search, where a user's unknown biometric template is searched against a database to identify that individual. An example of identification could be a

facial recognition biometric device installed at airport security to scan faces in the security line and search for matches of "persons of interest" loaded in a biometric database. However, this is an example of applying biometric technology for physical security, instead of logical access to computer networks or applications.

### UNDERLYING ISSUES

Tests that have been conducted on biometric technologies have included the False Reject Rate, which indicates the rejection rate of those users enrolled in the biometric that should have access, but are denied. This data is important in environments where positive access to the controlled area or system is paramount.

But perhaps more importantly, from

**For questions on biometrics or biometrics requirements, contact AFCA/WFP at DSN 779-5260 or visit the Air Force Communications Agency Biometrics section under Info & Services on the Air Force Information Assurance Web site:**

**[https://private.afca.af.mil/ip/info\\_services/ca\\_info.cfm](https://private.afca.af.mil/ip/info_services/ca_info.cfm)**



an information assurance perspective, is the False Acceptance Rate. That indicates the acceptance rate of users who are not enrolled in the biometrics that should not have access, but are authenticated. The FAR is difficult and often not feasible to measure on a comprehensive scale because what's needed is a large sample size of users not enrolled to test out the device to ensure access is not granted.

While security is a preeminent concern, users are also interested in how their biometric data will be protected. Currently, the amount of biometric data traversing the network is minimal. However, this is expected to increase in the future, while measures to minimize potential risk for exploitation and protection of data in transit and on storage services are still being researched.

### IDEAS ON HOW TO IMPLEMENT

Implementation of biometrics for logical access is still in the testing phase. However, the deputy secretary of defense outlined an enterprise vision for biometrics in August of 2003.

“By 2010, biometrics will be used to an optimal extent in both classified and unclassified environments to improve security for logical and physical access control.”

While the DOD and Air Force level policy and guidance is still in the

developmental phases, there is a clear sense that biometrics is the way ahead for providing increased information assurance.

Dr. John Woodward, director of the DOD Biometrics Management Office, recently conducted interviews with senior leaders from different military and government services on their perspectives on biometrics.

Perspectives on the benefits of biometrics for logical access included increased authentication and non-repudiation, monitoring insider threats or unauthorized use, potential cost savings when compared to maintaining UserIDs and passwords.

On the other hand, is there truly a requirement for biometrics as an added layer of security in addition to PKI or CAC, and what are the error rates for various biometrics technologies?

The Air Force Communications Agency, as lead command for Air Force biometrics, has an integral role in collecting and advocating biometric requirements from the field and working closely with the DOD biometrics management office on testing, standardization, and policy efforts.

Once this foundation is laid, biometrics appears to be a logical choice for logical access, another layer of security to protect critical information systems.

**Biometric technologies measure physical characteristics that include fingerprint and iris scans, hand geometry and facial recognition. Technologies that measure behavioral characteristics include signature verification and voice recognition.**

# OPERATIONS & EXERCISES

## require multi-level security methods

By Mr. Dennis Paquin

AF Agency for Modeling and Simulation

**ORLANDO, Fla.** — The need for all services, government departments, foreign states and coalition forces to train as one entity presents a major security and disclosure problem.

**Air Force leaders expect the warfighter to train as he fights and to be able to use all means possible to accomplish his goals, unhampered by old security concerns.**

Since Sept. 11, multi-level security methods of communication have taken center stage and old security work-arounds can't be tolerated.

Simulation training is done on stand-alone systems in physically separated locations to allow different classification levels to be worked in training and exercise events.

Information from different sources are then sneaker-netted to other systems for exercise inject.

Today's new exercise/training concept calls for interfacing geographically separated simulation systems (live, virtual, and/or constructive) into realistic training envi-

ronments. **A key challenge is how to link two or more simulations that operate at different security classification levels.**

The conventional approach is to operate the entire simulation at the highest security level of the participating exercises.

This limits play during Korean, NATO, and coalition exercises. It's also increasingly more difficult and impractical, and often limits training because it limits participation.

The future approach must be hinged on developing a multi-level security solution for distributed simulation.

**Multi-level security is the ability to work with information from all domains via a single workstation.** This would allow two or more classification levels of information to be processed at the same time within the same system, when some users are not cleared for all levels of information being used.

A number of initiatives are ongoing by many Air Force, service and nation-

al organizations. All are focused on a system that would allow use of all classified materials by different need-to-know personnel, with a password or physical card reader that would allow sign-on to the system— a security tag on information used during exercise or training events. The box would include a physical up-guard and a physical down-guard. These projects will in time solve the technical problem.

Progress also needs to be made on the procedures and policies associated with this effort. If the system is in a controlled environment then this would be the same as housing it in a Secured Compartmentalized Information Facility and not actually be multi-level.

The policy question is the hardest aspect. Policy must be changed to allow for true multi-level security. The National Security Agency sets policy for MLS. To change existing policy will take the full collaboration of the services, joint and national communities. To truly train as we fight, MLS must be a fully practiced reality.



# Reflections

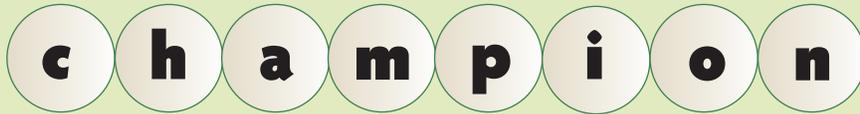
Mr. Robert Doubleday pauses to remember his father Maj. Gen. Daniel Doubleday, who is honored in the Ludwig Heritage Hall in the atrium of the Air Force Communications Agency at Scott AFB, Ill. He and his wife brought photographs and memoirs of one of the pioneers of modern communications during their visit recently. In the photo illustration, General Doubleday's portrait is located on the bottom left, and his photographic image has been added as a reflection facing his son. General Doubleday's career lasted from 1929 to 1963. Some of the highlights of his career included his assignment in 1943 to the United Kingdom and North Africa where he spearheaded the introduction of VHF communications. He also participated in the development of aviation communications and navigation equipment, including the first use of command radio sets in fighter aircraft, and the first instrument landing systems. Photo illustration by Mr. Gerald Sonnenberg

RECENT DEVELOPMENTS

**DMS TO BECOME WEB-BASED:** There's a new direction within the Air Force that's changing the way the Defense Message System is used. Enterprise Messaging-Air Force will bring significant changes to DMS from an end-user's perspective. No more DMS compliant Microsoft Outlook, no more FORTEZZA cards and PINs, no more X.509 forms to complete. Just the Internet Explorer Web browser and a Common Access Card is all people will need. For years, various commands, and some AUTODIN customers used a product called an Automated Message Handling System. The problem with the AMHS was that it did not understand how to handle DMS signed and encrypted messages. Now, through the efforts of commands and sister services, the AMHS has a new face —the CommPower XML Portal. The CP-XP is a "Front-End" to the AMHS and all the DMS messaging going in and out will be handled by it. Therefore, the Air Force can remove FORTEZZA cards and the DMS e-mail client from the end user's desktop. *(Master Sgt. Joseph Lucas, AFCA)*

**USAFE's PATCH NOTIFICATION:** Users throughout Europe will now have to ensure all security patches are installed in their computers before they can use them, according to United States Air Forces in Europe officials. They've begun an automated notice that tells people if they are in compliance with all security measures or not. What's different about this process is that users won't be able to access the network or logon until the required patches are installed. The concept was identified as a best practice at Spangdahlem AB, Germany, a year ago and is now being applied USAFE-wide. *(Ms. Linda Killman, USAFE)*

**ROBE's TRAINING FLIGHT:** Six aircraft from across the country met in the skies above the central United States Aug. 24 to conduct the first training flight of the Roll-on Beyond Line of Sight Enhancement communications system. The ROBE system allows an air operations center, command-and-control and strike aircraft to share a near-real-time ▶▶



**Growth through diversity: Positions available**

As of press time, 24 positions have been designated as part of the SCOPE Champion program, with steps being formulated to increase that number. When combined, these positions represent a cross section that helps candidates achieve increased breadth, depth, organizational and functional experience. Researching and examining these positions help illustrate how management reassignment may benefit one's career. For example, to work on organizational diversity, a candidate presently located in the Air Force Communications Agency might self nominate for the position located at the Air Force Reserve Command, should that position become available. A move like this may also result in functional progression, i.e. changing from a position that required technical expertise in the application of IT systems, to one that specializes in the management and direction of an Enterprise Information Management Program. The target audience is GS-13s through GS-15s (and their equivalents).

USTRANSCOM/J6	GS-301-15	Chief, Programs Division
AF/XIII	GS-343-14	Deputy Chief, Command and Control Integration Division
AF/XIIV	GS-343-15	Chief, AF Innovation Planning Division
AF/XIPS	GS-2210-15	Chief, Planning and Joint Actions Division
AF/ILCS	GS-2210-15	Chief, Command, Control, Communications & Computers (C4) Systems Division
AF/XIWA	GS-2210-14	Senior Information Technology Specialist
AF/XIWA	GS-2210-14	Information Technology Specialist
AFCA/CA	GS-301-15	Technical Director
AFCA/IT	GS-2210-15	Director, Architecture & Interoperability
AFCA/WF2	GS-855-15	Technical Advisor, Warfighter Integration
AFDPO/PP	GS-301-15	Director, Air Force Departmental Publishing Office
AFPC/DPKCI	GS-301-14	Communications & Information Career Program Manager
ACC/SCS	GS-301-15	Chief, Systems Integration Division
AETC/SCT	GS-2210-15	Chief, Architecture, Technology, & Interoperability Division & Technical Director
AETC/CSS	GS-391-14	Telecommunications Manager, Chief, Network Operations & Security Flight
AETC/SCX	GS-2210-14	Supervisory IT Specialist, Plans/Policy/Resources
AFFTC/IT (AFMC)	NH-4 (GS-15 Equivalent)	Interdisciplinary Position Deputy Director, Information Technology Directorate
ESC/DI (AFMC)	GS-301-15	Director, Information Management and Technology
AFRC/SCT	GS-2210-14	Chief, Architectures, Technology, and Interoperability Division
AFRC/SCX	GS-2210-14	Chief, Plans, Policy & Resources Division
AFSPC/LCOZ	GS-301-14	Chief, SATCOM Systems Branch
AMC/SCTE	GS-301-14	Chief, Enterprise Architectures Branch
PACAF/SCT	GS-301-14	Chief, Architecture, Technology, and Interoperability Division
USAFE/SCX-2	GS-2210-14	Deputy A6X/CIO Operations Branch Chief

— Source: Mr. Dan Thomann AFCA Civilian Career Force Executive Agent

common digital picture of the battlefield. The 40 ROBE-equipped tankers in Air Mobility Command, which will continue in their primary mission of air refueling, can act as relays for critical battlefield information. The Aug. 24 flight was just one of several that will occur prior to the ROBE's flight developmental evaluation in late September. (1st Lt. Michael Meridith, 319th ARW PA)

### INPUT NEEDED

**IDEA FOR DETECTION:** With Information Assurance and Computer Network Defense requirements and capabilities evolving at a lightning pace, Air Force Information Warfare Center personnel created the Intrusion Detection Exploration and Analysis facility. It has become the premiere evaluation facility for intrusion detection security systems.

The IDEA facility has a laundry list of who's who coming for support. Why? Some people want a little assurance from an independent analysis of various products. Others simply do not have the expertise or resources to adequately evaluate products. All want the best evaluation possible

before committing valuable resources and limited funding to purchase detection systems.

The facility consists of more than 48 different operating systems including all Windows, Linux, BSD, OS X and HP-UX platforms and the most advanced Cisco architecture equipment available. The environment was designed to evaluate new intrusion detection and intrusion prevention technologies at various bandwidth speeds. It can evaluate products from speeds ranging from T-1 (1.544 Mbps) to OC-192 (10 Gbps). Imagine moving the contents of a 3.5" floppy disk within 1-second, and then turn up the volume and move the contents of 14 CD-ROMs within one second ... that's fast. In a world of decreasing budgets, and downsizing of forces, stop and think of better ways to use valuable resources. Before heading down an endless road of IDS possibilities, remember some of the best IDEAs are right in front of you. (Capt. Steven Barker, AFIWC)

### SQUADRON WANTS YOUR TACTICS:

The ancient Chinese warrior Sun Tzu once said "the terrain drives tactics,"

and that certainly still holds true today. Today the terrain is the comm and info network the enemy uses, and there are plenty of enemies ... a script kiddie here, a student hacker there and don't forget state sponsored hacking. They all provide the depth of this virtual terrain.

Defense tactics come into play when a situation presents itself within certain parameters, and a comm warrior must make an on-the-spot decision on how to save the network. Much like a fighter pilot taking a hard bank to drop a certain type of munition, the comm warrior takes similar actions in Computer Network Defense. The 23rd Information Operations Squadron at Lackland AFB, Texas, provides these tactics to you, the comm war fighter. But they can only do their job with your help, as these tactical situations must be gleaned from the field.

If anyone feels a tactic merits publishing to the rest of the comm community, submit a Tactics Improvement Proposal on an MC Form 1007 or an AF Form 4326. They're the same forms the pilots use in the air warfare community. You can also submit it online:

<http://iwttactics.afwc.aia.kelly.af.smil.mil>. Once the TIP is submitted, a team researches it and executes a Tactics Development Initiative, or TDI.

TDIs are normally very focused in scope, addressing one specific area of the proposed tactic. Once the execution phase is over, the tactic is published in the Tactics, Techniques and Procedures Manual AFTTP 3-1 Vol. 36. AFTTP 3-1 has volumes for every weapons system the Air Force employs. There's one for B-52's, F-117's, even the AWACS. Volume 36 happens to be the Information Warfare volume. See, the comm community really is part of the combat force.

Just ask any fighter or bomber pilot how Information Operations fits into the overall fight and chances are he or she will mention a tactic or two that's documented in Vol. 36.

If you have ever been sitting around your operations floor, thinking, "what if we do this ...?" stop for a moment, write it down and submit it to the 23rd. Who knows, you may be the next warrior to discover an entirely new tactic. (By Tech. Sgt. John Schuler, 23rd IOS)



Senior Airman Priscilla Robinson / 31st CS

**TEAMWORK:** The 603rd Air Control Squadron, a deployable communications unit, sets up a mobility tent as part of a Survive to Operate training class held at Aviano AB, Italy. The 603 ACS directs, controls, and coordinates United States Air Forces in Europe and NATO air and space operations collecting and evaluating tactical information to provide a fused, real-time air picture to theater commanders.

## KUDOS

**MAGAZINE EARNS AWARD:** The Air Force Communications Agency's *intercom* magazine was recognized with a Clarion Award as "Most Improved Magazine, Internal Publication," as well as an honorable mention as the "Best Overall Internal Magazine." Specifically mentioned in the award were Master Sgt. Karen Petitt, managing editor, and Tech. Sgt. Jim Verchio, editor.

The Clarion Awards are sponsored by the Association for Women in Communications. The AWC sponsors an international competition with awards in more than 90 professional categories. The competitors, which include publications such as *Time* and



*Newsweek*, are recognized for their excellence in communications. The competition is also designed to show how modern communicators demonstrate competence in varied disciplines and are able to network and make career moves across the broad spectrum of communications fields. Disciplines represented within

the association include: print and broadcast journalism, television and radio production, film, advertising, public relations, marketing, graphic design, multi-media design, and photography. (Mr. Gerald Sonnenberg, AFCA/PA)

**EXCELLENT RATINGS:** The 55th Wing at Offutt AFB, Neb., earned an excellent rating for information protection and the Information Assurance Team received a Superior Performance Award for the wing's Operational Readiness Inspection. The wing, which has the fifth largest of 16 LANs in the Air Combat Command Enterprise Network, has not had a classified message incident in more than four months, and has maintained time

compliance network orders for workstations at more than 95 percent, and 100 percent for servers. This is due to the IA team's extensive education efforts to more than 800 troops about compliance, password protection and virus prevention, and their ready-made training reminders for troops deploying. (Master Sgt. Jacquelin Conley, 55th CS).

**CUSTOMER PROFESSIONAL:** When you work in a Wing Information Assurance office, sometimes you feel like a mixture of the information section at a library, an extension of the Help Desk, or the messenger who is about to get shot. It's all worth it though for Ms. Mary Smith who helped launch Mountain Home AFB,



Staff Sgt. Adrian Cadiz/ 3d CS

**Flag raising in Kirkuk:** Master Sgt. Lawrence Paquette presents the 506th Expeditionary Communications Squadron guidon as squadron members present arms during the raising of the U.S. Flag at Kirkuk Air Base, Iraq, Sept. 13. The flag is raised and lowered every Monday morning at the 506th ECS work compound prior to their weekly awards presentations.

Idaho's IA Awareness and Assessment Program visits. It's not just meeting with a few customers a day and talking to a bunch of others over the phone or through e-mail, but meeting the customers, in large numbers, out where they work.

Ms. Smith, the Assistant Wing IA manager, said her favorite times are meeting with new unit reps and seeing the light of understanding in their eyes, and seeing their IA programs and documentation blossom in a matter of days.

One unit rep said, "I knew I had to keep track of all these different things, but now I see how they really all fit together!" For the newer folks, Ms. Smith will conduct an initial visit to go over the checklists and make sure they understand what the IAAP covers. Then, she'll conduct the actual assessment visit, and sometimes she visits a third time if they weren't able to get it right. When their program comes together and Ms. Smith approves it, they know that they are the ones to get it done and they're proud of that fact. Ms. Smith works hard to make it a positive experience for them, and as a result she feels great about it as well. (Ms. Terry Pobst-Martin, 366th CS)

**ACC NOSC GUARDS:** Through remote centralized management, the Air Combat Command NOSC controls configuration changes, patch distribution, virus protection, and many other boundary protection tasks. The security monitoring tools allow the NOSC to present the status of the network in real time.

Standardization helps provide consistent service to all of their customers, speeds troubleshooting, and increases system availability by reducing downtime. Specialized NOSC teams have fewer tasks to track, and are less likely to miss potential security vulnerabilities in the ACC network. Because of the NOSC dependence on remote servers and networks, there's an increased security vulnerability and operational risk. Just one vulnerable system can provide a foothold to accessing the entire enterprise network.

Centralized Management allows

them to keep system patch levels standardized and current thereby reducing their exposure to would-be intruders. When a new vulnerability is identified, the NOSC can quickly determine how many of their bases are affected and develop a course of action to contain and repair the damage to their network, as well as protect from any further attack. Specialized training costs can also be reduced with centralized management. Training the number of people that it takes to have a fully qualified boundary protection team at each warbase consumes much more time and money than having one fully qualified NOSC team. The money saved can be used for new technology,

and the base-level technicians can devote more time to handle customer issues local to the base community. (Airman 1st Class Alisa Castro, 83d CS)

**POSTAL WARRIORS:** When was the last time you witnessed a postal worker strap an M-9 pistol to his hip or sling an M-16 rifle over his shoulder and hop a ride on a Black Hawk helicopter? As dramatic as it sounds, it's reality in the Iraqi hot zone. Postal troops riding as war fighters on a convoy from base to base are not uncommon in daily operations. It puts a warrior spin on every postal worker's job. At any given moment, they rely on previous training that one day could save

their life or the life of the person next to them.

Such is the case for Det 1, 82nd Communications Support Squadron members. Progress with the mail centers in Iraq has increased exponentially in a very short amount of time. Air Force and Army postal workers are working under one umbrella and redefining teamwork. Also comprising a significant part of the work force are the brothers in blue from the Information Management corps. We are now taking "file clerks" and "pencil pushers" and carving them into Postal Warriors. Workcenters have been lauded with positive comments and feedback from the troops. The mail must get through, whether letters, packages or ballots and the Military Postal Team will continue to deliver its precious cargo. The country's war fighters expect nothing less. (Staff Sgt. Andrew Gierza, 82nd CSS)



Senior Airman Kevin Camara / 2nd CS

**PENTAGON CHANNEL:** Tech. Sgt. James Jewell, and Staff Sgts. Chad Hearne and Mike Collins install and align a satellite dish that will allow the newly renovated Barksdale Commanders Access Channel to receive the Pentagon Channel, which is broadcast from Washington, D.C. They're with the 2d Communications Squadron at Barksdale Air Force Base, La.



**POSTAL WORKERS KEEP THE MAIL MOVING**



# PUBLIC KEY ENABLING

## What is it?

People preparing for TDYs are now required to use the Defense Travel System online, at their desktop, to process their orders. This Public Key-Enabled system requires a person to use their Common Access Card. DTS is among a growing number of everyday, mission-oriented applications that are taking advantage of the benefits Public Key Infrastructure brings by enabling their applications to use the PKI certificates for access, identity verification, and to protect the information resources.

## Why do we need it?

The Air Force is committed to achieving Information Superiority through a highly interconnected, network-centric environment and a key to this is the benefits of PKE to improve security of systems and networks. During the past two years the Air Force's focus has been on converting identification cards to the CAC, and providing the middleware and card readers needed to access and use PKI certificates. Those objectives have been achieved, and the Air Force is now moving to the next frontier, PK-enabling of networks and applications.

PKI provides for interoperable security services including authentication, data integrity, and confidentiality, and supports digital signature, access control, and non-repudiation. Everyone uses their CACs at least once each duty day when entering a base. As the Air Force moves into the use of PKI certificates as part of its net-centric business practices, people will use many tools.

## PKE and network enabling

One of the tools for network enabling is Smart Card Logon. Smart card certificate-based logon provides the advantage of allowing users to be authenticated with something they know (Personal Identification Number) and something they have (CAC with DOD PKI certificates). The users are not required to remember their network passwords. The certificate used is currently the e-mail signing certificate on the CAC.

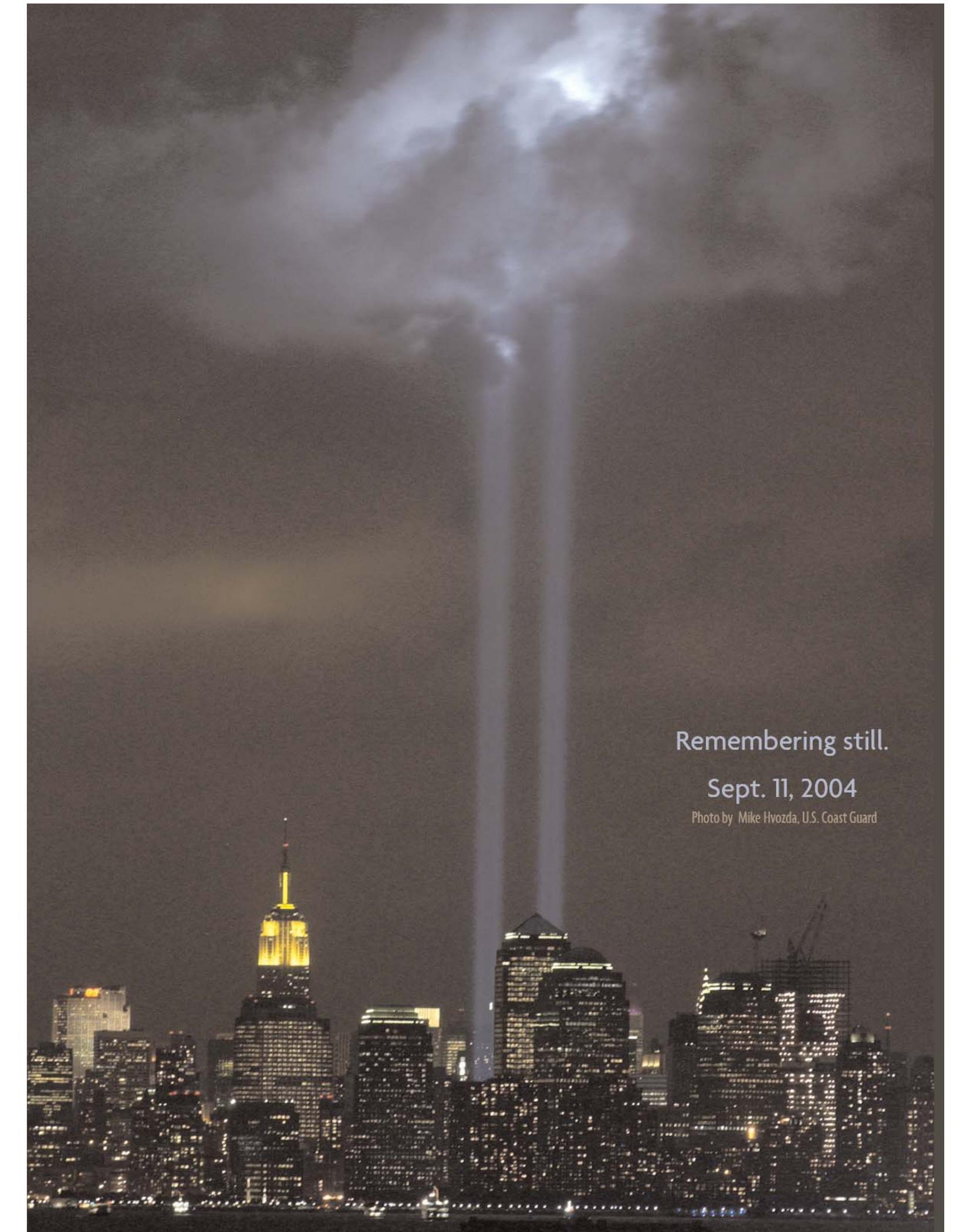
## Problems addressed with PKE

As SCL is being implemented by major commands across the Air Force, one particular problem continues to surface, logon failures due to certificate errors. Air Force PKI officials are devising a solution to help users determine CAC readiness for SCL. Until then, CAC holders can help make the implementation go smoother by

- ▶ verifying that the e-mail signing certificate was issued after May 18, 2002;
- ▶ the e-mail address is correct; and
- ▶ that the e-mail signing certificate is set as the default certificate.

Another area being addressed is users forgetting their CAC's PIN and locking the CACs. To address this issue and aid the transition to more usage of the CAC, the Air Force is fielding a CAC PIN Reset capability. The CPR system was developed as an alternative to the Military Personnel Flight for unlocking CACs and providing users with an on-site capability to reset their PINs.

SOURCE: AFCA/WFP Information Protection



Remembering still.

Sept. 11, 2004

Photo by Mike Hvozda, U.S. Coast Guard



“An invasion of armies can  
be resisted, but not an idea  
whose time has come.”

-Victor Hugo

# intercom

Journal of the Air Force C4 community ☆ October 2004



Warfighters depend on

## **INFORMATION ASSURANCE**

- ▶ The three pillars of IA ▶ Defending the networks
- ▶ Confidence in emission security ▶ Viruses & hackers