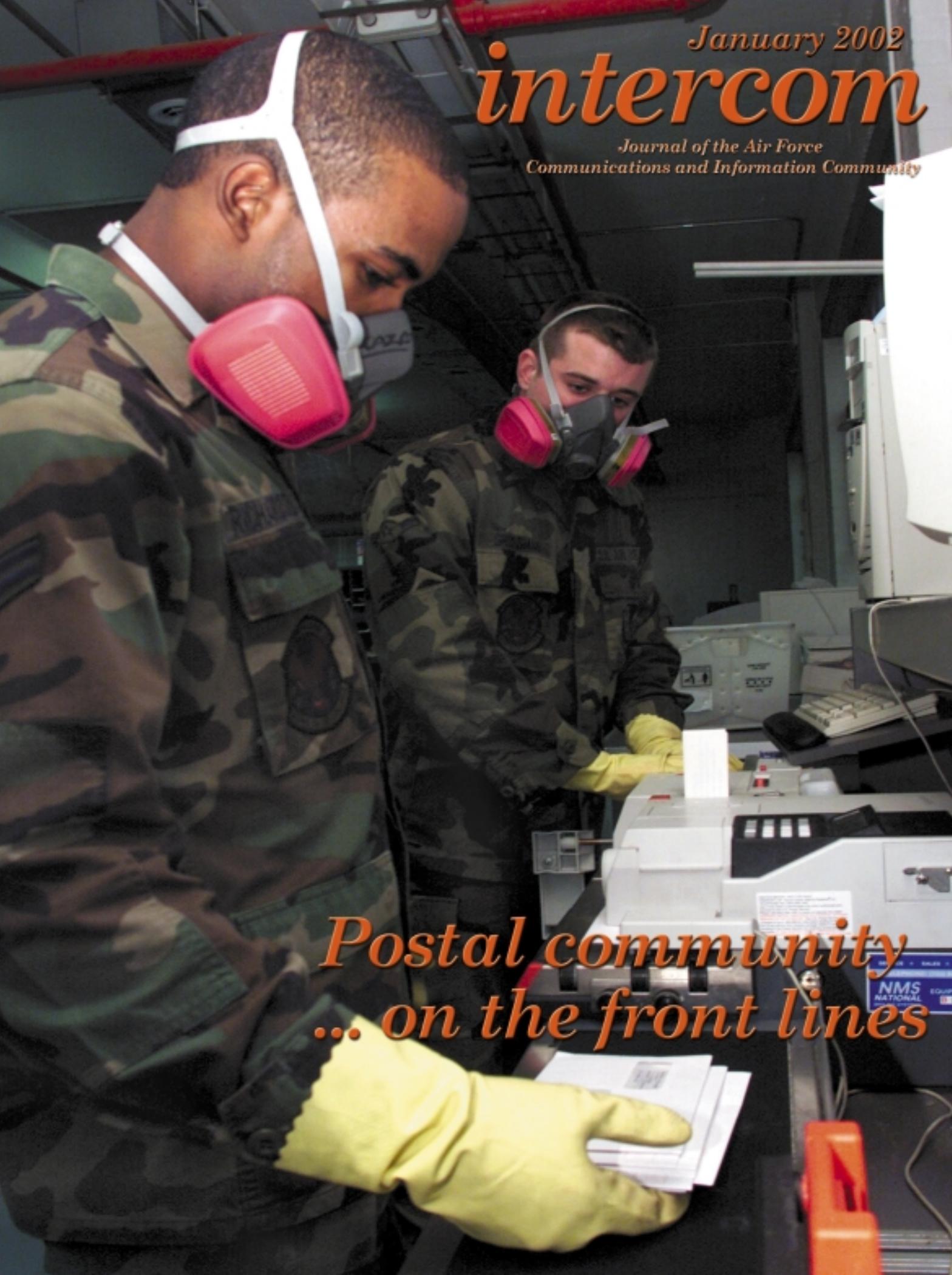


January 2002

# *intercom*

*Journal of the Air Force  
Communications and Information Community*

A photograph of two military personnel in camouflage uniforms and respirators working at a computer workstation. The person in the foreground is wearing a pink respirator and yellow gloves, holding a stack of papers. The person in the background is also wearing a respirator and yellow gloves, looking at a computer monitor. The workstation includes a keyboard, mouse, and various pieces of equipment.

*Postal community  
... on the front lines*

# intercom

Volume 43, No. 1

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

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

Editorial Staff

AFCA Chief of Public Affairs  
Lori Manske

Executive Editor  
Len Barry

Editor  
Tech. Sgt. Michael C. Leonard

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

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

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

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

News copy, photos, story ideas and comments may be e-mailed to [intercom@scott.af.mil](mailto:intercom@scott.af.mil), or mailed to AFCA/XPPA, *intercom*, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222. Fax is DSN 779-6129 or (618) 229-6129. Editorial staff may be contacted at DSN 779-5690, or (618) 229-5690.

Check out  
our Web site at:

<http://public.afca.scott.af.mil/>



## postal community ... on the front lines

- 4 Air Force Postal System: First-class service, first-class people
- 7 Air Force explosive detection technology enhances mail security, force protection
- 8 Hurlburt mail handlers equal to terrorism challenge
- 10 Handling mail: A force protection issue that involves everyone
- 12 11th CS safeguards mail for Pentagon, Bolling
- 14 ACC postal services combat America's bio-terrorism threat
- 16 Edwards' BITS forms first line of defense



- 18 PACAF postal service protects your mail
- 21 Thule heightens mail handling security

## IA: contingency planning for GSTF



- 23 System availability in war represents ancient requirement, modern challenge
- 25 Protecting critical infrastructures key to IA
- 28 How important is your data?

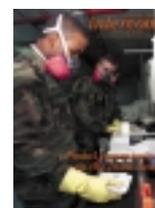
## in other news

- 32 Theater deployable communications makes vital contribution to Operation Enduring Freedom
- 35 Counsel's corner



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

### On the cover



Airman 1st Class  
Jazzreal Richardson  
(left) and Airman  
Nicholas Grossman,  
11th CS, meter  
outgoing mail.

Photo by Staff Sgt.  
Brian M. Boisvert, 11th CS

# Information Assurance campaign: Keeping the fire lit in 2002

By Lt. Gen.

**John L. Woodward Jr.**

*Air Force Deputy Chief of Staff  
for Communications  
and Information  
Washington*

Last year we put a blitz on IA awareness and eliminated a multitude of IA vulnerabilities through the IA campaign. Twelve monthly themes focused our attention on a succession of important IA issues: from “Roles and Responsibilities” to “Threats and Countermeasures” ... from “Digital Devices” to “Computer Network Defense” ... from “Web Security” to “IA in the Expeditionary Aerospace Force.” Our collective knowledge in these areas has significantly improved. Many network vulnerabilities

were also eliminated through aggressive problem identification and resolution, and the use of IA tools.

We covered much ground last year, but our campaign is far from complete. More awareness and network protection actions are necessary before we can declare victory for the IA campaign.

In 2002, we must focus on IA activities directly supporting the war on terrorism. Our new campaign theme reflects this focus: “Defeating Global Terror ... Demands Effective Information Assurance.” This year, several operationally-oriented IA themes have been planned, including “Contingency Planning, Operational Security, Remanence Security (Sanitization and Destruction),” and “Vulnerabilities and



**General Woodward**

Incidents.” We will also revisit some important 2001 themes, such as “Web Security, User Responsibilities,” and “E-mail.”

I highly encourage everyone to become fully engaged in the continuing IA campaign. We must keep the fire lit ... the warfighters depend on us!



## *Air Force Communications Agency kicks off IA Campaign 2002*

By Col. Thomas J. Verbeck  
*Commander*

*Air Force Communications Agency  
Scott AFB, Ill.*

Air Force Communications Agency kicks off our Air Force Information Assurance Campaign 2002 this month with the theme, “Information Assurance Contingency Planning for the Global Strike Task Force.”

With increasingly greater warfighter dependence on our Air Force computer networks, it’s crucial we be ready to deal effectively with interruptions to global network operations. There are clear measures and steps to follow in contingency planning to ensure we continue to function in the face of either accidental or deliberate disruptions.

I invite you to carefully read, then adopt the principles in the articles in this issue, and monthly

issues to come, on applying Information Assurance contingency planning to all aspects of the Global Strike Task Force. We must be prepared to deal with events affecting information operations both large and small -- from power outages, hardware failures, fire and storm, to hacker and virus attacks. Information Assurance contingency planning not only makes good business sense, but also helps to assure constant Information Superiority and decision dominance for our warfighters.

I urge your attention to Information Assurance considerations in every aspect of your daily duties not only this month, but throughout the year ahead. With a united and concerted effort, we’ll succeed in helping to maintain the world’s greatest Air Force at peak capability and readiness.

**For more  
Information  
Assurance  
articles,  
see  
Page 23**

# Air Force Postal System: First-class service, first-class people

**By Robert Eichholz**  
*Air Force Postal Policy Chief*  
**and Chief Master Sgt. Todd Small**  
*Air Force Postal Career Field Manager*  
*Pentagon*

Have you ever wondered how those packages from Aunt Jenny or Uncle Joe, mailed from some small town lying an ocean away, arrive at bases overseas? Or perhaps, how that piece of official correspondence shows up on your desk? Well if, as they say on the popular game show, “No” is your “final answer,” then you’re probably not alone. In fact, we suspect few folks stop to ponder just how that smiling airman behind the counter of your local air post office came to possess that care package from home.

In a typical year, postal warriors serve nearly one million patrons, including 200,000 on deployment. They also receive, process and dispatch more than 200 million pounds of mail and conduct more than \$35 million in financial transactions.

Unlike the other military services, the Air Force doesn’t classify personnel performing postal duty into an enlisted specialty, or include postal as part of the normal career progression of any Air Force specialty code. On April 30, 1977, the postal special duty was created when administrative specialists, AFSC 702X0 (now 3A0X1), serving in Air Force postal activities were converted to the 99604 postal special duty identifier (now 8M000). Today postal personnel come from many Air Force walks of life, such as aircrew life support, supply systems analyst, air transportation, munitions systems, services, personnel, and health services management.

Air Force postal specialists hold a position of tremendous trust with both the U.S. Postal Service and their customers. By agreement of the USPS and the Department of Defense, personnel who perform postal duties must be loyal, trustworthy and honest. These individuals provide postal finance services, including the sale of stamps and stamped paper; issuing and cashing domestic money orders; and providing certified; insured and

registered mail services. In fact, the average APO has a postal account valued at about \$25,000. All funds associated with, generated by, or exchanged during the normal course of postal activities belong to the USPS. Accordingly, postal personnel are held individually accountable for funds under their control. Postal personnel must reimburse the USPS for any fund shortages found in their accounts after audits. Personnel are also required to have security clearances to enable them to process and handle registered mail.

Because of this special trust, postal personnel are required to demonstrate responsibility both in the management of their personal finances and their personal conduct. Simply put, personnel of questionable integrity may not be assigned to duties in military post offices, mail centers, mail terminals or other postal facilities. Any derogatory information or unfavorable conduct that casts doubt on the military member’s trustworthiness and honesty makes them ineligible for postal duty. The Air Force rigorously enforces the high standards established by the USPS and DOD.

Postal duty also requires extraordinary physical effort and demands personal sacrifices. The unending, constant flow of mail, coupled with precise financial and registered mail accounting requirements, often mandate that postal operations continue long after customer service windows are closed. As the end-of-year holiday season approaches, a time when many military personnel are looking forward to minimum manning, reduced work schedules, and spending time with their families, an already demanding postal operations tempo hits its peak. In fact, most postal personnel are prohibited from taking leave during the mail rush that begins before Thanksgiving and continues well into the new year. While postal service is always deemed an important quality of life issue, it takes on special significance during the holidays, as gifts and letters are exchanged between military members and their loved ones. A doubling or tripling of the normal mail volume is common during this time.

At certain locations, Air Force postal workers

# Mail Movement Between CONUS and Overseas



operate in a hostile or high threat environment, wearing flak jackets and driving armor-plated vehicles. In many locations, they must constantly change their mail delivery and receipt procedures and driving routes because of the ever-present threat of terrorism. These variations in mail dispatch and receipt procedures are essential to force protection, personal safety, and protection of the mail. At some locations, postal personnel may be the only in-country Air Force enlisted members, or the sole Air Force representatives. As a result, postal personnel often operate autonomously, independent of normal Air Force supervision, and routinely assume great responsibility, representing the Air Force and military postal service in meetings with foreign postal officials.

As with any Air Force specialty or special duty, training is a paramount consideration and one of the keys to operational success. Personnel selected for postal duty attend the DOD Basic Postal Course at Fort Jackson, S.C. Prospective postal personnel from all service branches attend this four-week course taught by the U.S. Army's Adjutant General School. Postal supervisors also attend a 10-day Postal Supervisor Course at Fort Jackson.

Despite the advent of technology and e-mail, postal mail volume continues to increase rather than decrease. The USPS handled nearly two billion pieces of mail in 1998, as documented in its annual report (up from 1.9 billion in 1997, and 1.83 billion in 1996). In fact, the impact created by tech-

nology, particularly in the area of e-commerce, is being felt by MPS. With online ordering at an all-time high, postal personnel are working hard to plan for and accommodate increased workload brought on by military customer purchases as they flow through USPS into the APO system. Reengineering, force modernization, and policy changes have also increased the amount of mail being managed by MPS.

Postal personnel directly impact both mission success and morale. While this impact is evident in-garrison, it's most apparent in deployments, contingencies and combat operations. Anyone who's spent time in a deployed environment can relate to the absolute criticality of official mail service, as well as the personal importance of a "care package" from home.

Speaking of care packages, you're probably still wondering just how that package actually makes it to you ... an ocean away. Here's a thumbnail scenario:

Let's say Aunt Jenny and Uncle Joe want to send you some candy, cake, toiletries, powdered drink mix, or just a clean pair of socks. It has to get to you fast, so they airmail you a package from their local U.S. post office (any one of 38,000) to an overseas APO. The U.S. post office trucks all the mail they accepted that day to a regional postal

See **MAIL** Page 17

# Military postal system's history reflects ability to adapt to changing environment

By Robert Eichholz  
*Air Force Postal Policy Chief*  
and Chief Master Sgt. Todd Small  
*Air Force Postal Career Field Manager*  
*Pentagon*

The Air Force Postal System is an integral part of the Military Postal System that stems from Article 1, Section 8, of the Constitution. The Constitution provides that Congress shall have the authority to establish post offices. Acting under this authority, Congress established the U.S. Postal Service and granted it absolute monopoly in providing postal service.

Within the military, the Naval Postal System was established by an act of the 60th Congress in 1908. In 1912, this act was amended to include provisions for the Marine Corps. The act was again amended in 1941 to include the U.S. Army Postal Service.

In 1953, the 6005th and 7025th Air Force Postal and Courier Groups were activated under Pacific Air Forces and U.S. Air Forces in Europe respectively. The major commands managed operations through a series of detachments and operating locations reporting to the groups. This continued until 1966, when the U.S. Air Force Postal and Courier Service was established. Headquartered in Washington, this organization managed operations through a series of regions and districts, and commanded 487 activities in 60 countries. It was deactivated in 1976. Postal management functions were realigned under each MAJCOM director of administration. This established air postal squadrons that maintained operational and administrative control of postal services until 1994.

In 1994, post offices were assigned to each wing's mission support squadron under the "one base, one boss" concept. MAJCOM postal staffs were realigned as direct reporting units. In 1996, the communications and information community and information management community merged, and with the merger, postal became part of communications and information. This alignment remains in place today.

Air Force postal activities play an important role in MPS, which is the responsibility of the Department of Defense, under agreement with, and



*Photo by Staff Sgt. Chuck Marsh*

**Airman 1st Class Kenneth Taylor (left) and Staff Sgt. Toni McKinney, postal workers at the RAF Mildenhall post office in England, check the addresses on a shipment of magazines.**

as an extension of, USPS. MPS provides full postal services for all DOD personnel, family members and other authorized personnel beyond the boundaries of U.S. sovereignty, and where USPS service is nonexistent. Today there are nearly 650 Air Force postal specialists on duty at 123 air post offices and 13 aerial mail terminals and mail control activities around the globe supporting MPS. The Air Force also provides postal specialists to five joint military postal activities and the Military Postal Service Agency.

As these changes have occurred over the past century, the goal of our military postal organization remains to provide world-class service to military and family members overseas.

# Air Force explosive detection technology enhances mail security, force protection

## Air Force Postal Policy Element

WASHINGTON, D.C. – Air Staff postal officials are introducing state-of-the-art technology to the age-old practice of processing military mail. At a cost of nearly \$7 million, the Air Force began fielding ion mobility spectroscopy instruments in October and will continue through May. Eventually all air post offices, aerial mail terminals, and selected stateside official mail centers will operate the equipment. The systems will be included in Air Force postal deployment kits used during contingencies.

These field instruments, often called “chemical sniffers,” are adaptations of laboratory equipment. IMS detection of explosives is not really a chemical method, but rather a physical comparison.

The instruments vaporize a sample, converting molecules to ions, and analyze the molecules by electronically comparing them with data pre-programmed by the manufacturer.

“After a thorough review of existing research, it was clear no single technology is effective in identifying all potential vulnerabilities,” said Robert Eichholz, chief of Air Force Postal Policy. “But widespread use of this type of system in places such as airport and diplomatic security checkpoints, as well as the Pentagon’s remote distribution facility, convinced us it was the right approach,” Eichholz said. “These systems can detect both narcotics and explosives, but because of U.S. laws against unauthorized search and seizure, our use will focus solely and specifically on explosives.”

Anti-terrorism and force protection assessments have recommended mail systems use available technology to assist in screening deliveries for explosives. “Immediately after the events of Sept. 11, Lt. Gen. John L. Woodward, Air Force deputy chief of staff for communications and information, tasked us to find a credible and effective way to



**Staff Sgt. Nakia Arrington, U.S. Air Forces in Europe Air Postal Squadron, uses ion mobility spectrometry equipment to screen a parcel for explosives.**

improve security of mail and Air Force postal facilities,” he said. “We benefited tremendously from efforts of the USAFE Air Postal Squadron, who’ve been pursuing this kind of equipment for nearly two years after the Aviano mail incident,” Eichholz added. In February 2000, an Aviano airman suffered minor injuries when a parcel he received through the American military postal system detonated upon opening.

Although deployment of these systems will take several months, approval to acquire them came quickly. “Because of the pressing need to protect the mail, our people and Air Force facilities, we were able to use the rapid response process to expedite approval of our request for these systems,” said Chief Master Sgt. Todd Small, Air Force career field manager for postal. The Air Force’s rapid response process uses a combat-mission needs statement to quickly document and staff urgent requirements. “We were able to move out quickly, with approval for purchase coming just a few weeks

See **DETECTION** Page 17

# Hurlburt mail handlers equal to terrorism challenge



**Frank Spann, 16th Communications Squadron postal employee, properly inspects Hurlburt Field's packages before they're sorted.**

**By Master Sgt. Larry Hernandez**  
*Base Official Mail Manager*  
*16th Communications Squadron*  
*Hurlburt Field, Fla.*

When it was announced that people were getting sick and even dying from being exposed to anthrax contamination in the mail, mail handlers in the Hurlburt Field post office initially experienced fear and anxiety. They talked among themselves, wondering who was responsible and why. They feared this might be only the beginning, and that there were more attacks to come. Though

many weeks have gone by and some of the fear and anxiety has subsided, the anthrax threat remains – both in the news and the minds of mail handlers – and postal workers continue to take measures to protect themselves and their customers.

Recent events re-emphasize the importance of responding in an appropriate manner to provide early intervention. The Hurlburt post office has taken an active stance by remaining vigilant, alert and informed of latest developments on mail handling and processing.

Immediate actions are taken to minimize exposure to anthrax and detect explosives. Security forces screen mail delivery trucks at the base gate with explosive detection equipment or canine dogs before allowing them to enter. Contract postal workers manually and visually screen, handle and sort the mail. The Air Force has purchased explosive detection scanners for issue to the field, and Hurlburt Field has been designated a recipient. While this equipment won't be a 100 percent solution, it will significantly enhance our capabilities.

The Hurlburt Field post office consists of three separate, distinct and collocated entities: the base information transfer center, the postal service center, and the U.S. Postal Service. Twelve civilians and three airmen currently work in the post office, with approximately

4,000 pieces of mail handled daily. However, with the anthrax threat, there's no distinction between official and personal mail – any piece of mail might be contaminated.

This post office has taken steps to minimize exposure to its employees. The postal contractor has made professional protective equipment available to all mail handlers – including disposable gloves, face-piece respirators and protective gowns. Additionally, mail handlers are made aware of the importance of being vigilant and alert for suspicious mail. They're continuously kept informed of anthrax related issues, through advisories provided



*Photo by Senior Airman James Davis, 16th Special Operations Wing*

**Robert Renfro, (right) and Leroy Sumter, postal workers from the 16th Communications Squadron, carefully examine packages before sorting them.**

by the Centers for Disease Control and Prevention, FBI, Department of Defense, USPS, and Hurlburt's 16<sup>th</sup> Medical Group. A read file containing all these issues has been established as an ongoing reference.

Characteristics of suspicious mail and instructions to follow when it's discovered are posted throughout immediate work areas. The information was also provided to activity distribution offices throughout the base, since commercial carriers deliver packages directly to the unit.

Finally an alternate location for postal operations has been designated, in case the Hurlburt post office is incapacitated for any reason. A fully functional and complete paragon mail system is in place, along with postal supplies, computers,

**Carol Milligan, 16th CS postal worker, wears protective gear while sorting Hurlburt Field's mail.**

copier, mail bins and other items.

Use of anthrax as a terrorist weapon is a new threat to our nation. But whatever the threat, America stands united and ready to overcome it. The Hurlburt Field post office will do its part by ensuring the mail continues to flow quickly and safely.



# Handling mail:

A force  
protection  
issue that  
involves  
everyone



*Photos by Staff Sgt. Norma J. Martinez*

**From left: Airman 1st Class Aaron Edgar, Airman  
Melissa Jourdain, and Airman 1st Class Tiana**

**Williamson wear gloves and masks as they sort  
the base mail.**

**By Master Sgt. Dave Osborne  
and Master Sgt. Quincey Harrison**

*Official Mail Managers*

*Directorate of Communications and Information*

*HQ Air Mobility Command*

*Scott AFB, Ill.*

They've hardly been known – those warfighters who process and deliver military mail. They've normally gone virtually unnoticed in the great scheme of Air Force daily activities – that is, until now. Today base information transfer center warriors perform their jobs on the front lines of homeland defense in America's war against terrorism. The events of Sept. 11 transformed our world, including mail processing. Letters laced with anthrax, and the threat of other biological agents, caused BITC personnel to alter the way mail is handled and processed.

After anthrax letters were identified in the U.S.

Postal System, Air Mobility Command BITC personnel increased their protective posture by wearing gloves and masks for processing mail.

Bioenvironmental engineers conducted health risk assessments at each AMC BITC, to help identify vulnerabilities, and to ensure individuals were prepared and educated on proper wear of personal protective equipment to cope with the current threats. Another level of protection will be added in February, when 11 AMC bases receive Barringer 400B ION scanners. These systems will provide an extra layer of screening and security for mail processing. The scanners can detect explosives and narcotics, and are deployed in more than 40 countries around the world to enhance aviation security, protect high profile facilities, help prevent terrorist attacks and assist with drug interdiction.

Air Force BITC personnel act as military ambassadors to the U.S. Postal Service, and continue to nurture an outstanding working relationship.

They interact daily with USPS employees who screen mail prior to delivery to BITCs, which now routinely receive USPS information, guidance and updates on anthrax and the current threat. Information is relayed to activity distribution offices in each organization. ADOs apply the same level of heightened awareness in screening and processing, which adds another layer of mail protection.

On a broader scope, for protection of our families and ourselves, each of us needs to follow BITC guidelines to

scrutinize personal mail delivered to our homes by USPS and private carriers. We need to answer the same questions BITC and USPS personnel ask themselves when handling each piece of mail.

- \* Does it have a return address?
- \* Do you recognize the return address? Does it appear to be fictitious?
- \* Is it properly addressed?
- \* Does it have oily stains?
- \* Does it have protruding wires?
- \* Were you expecting it?
- \* Does it contain excess postage?
- \* Does it have restrictive markings, such as “personal” or “confidential”?
- \* Is the postmarked city different from the return address city?
- \* Is it lopsided or lumpy in appearance?
- \* Is it sealed with excessive amounts of tape?

If you receive a package exhibiting any of these traits, treat it as suspicious – whether it’s government official or personal, delivered by USPS or a private carrier.



USPS has taken measures to combat the threat and minimize risks. The federal government has authorized USPS to purchase



**Staff Sgt. Tammara Lamar, NCO in charge of BITS, explains how to spot a suspicious package to Airmen Edgar, Jourdain and Williamson.**

equipment to “zap” or sanitize the mail. Deployed throughout the U.S. at large mail processing centers, these systems will sanitize mail before it’s delivered to district post offices for processing by individual letter carriers.

The current risk of exposure to anthrax or another biological agent transported in military mail is low. To date, only seven suspicious items have been identified and reported within AMC. Compared to the quantity of mail handled and processed each day at every AMC BITC location, this is a very low figure. All seven items tested negative for anthrax, other biological agents and explosives. We can continue to reduce our risk of exposure by using heightened scrutiny and security measures, following Air Force and USPS addressing formats, and applying a common sense approach to mail handling.

BITCs and USPS continue to provide customers information and guidance for properly identifying, handling and reporting suspicious mail. As individual citizens, we can and must do our part.

AMC BITC warriors are proud of their work and take it seriously. They do an outstanding job of handling and delivering military mail in a manner that contributes to homeland defense.

However, safe handling of mail is more than a postal concern – it’s a force protection issue. All Air Force personnel have a responsibility to do their part to assure our mail is secure and safe to open.



## **11th CS safeguards mail for Pentagon, Bolling AFB**

*Photos by Staff Sgt. Brian M. Boisvert, 11th CS*

**From left: Airman Nicholas Grossman, Airman 1st Class Roland Jones, Airman 1st Class Jazzreal Richardson and Airman 1st Class Scott Molnar,**

**11th Communications Squadron, load a BITC truck with outgoing mail to be taken to the U.S. Post Office for dispatch.**

**By Carolyn Price**  
*Chief, Support Flight*  
**and Lt. Col. Gregory Edwards**  
*Commander*  
*11th Communications Squadron*  
*Bolling AFB, D.C.*

We salute the 11th Communications Squadron's mailroom staffs for their role in the front line of defense against potential anthrax attacks at the Pentagon and Bolling AFB, D.C. In light of the threat, they've taken steps to identify suspicious mail. Extreme vigilance and caution must be exercised when processing mail, especially when it's to be delivered to senior Air Force officials. Chemical protective gear includes gloves made of vinyl and nitrile, a high-grade industrial plastic. In addition, goggles and masks filter out 95 percent of microbes in the air, including anthrax spores. Sorting bins and distribution equipment are cleaned daily with a chlorine bleach solution.

Mailroom supervisors attended several train-

ing sessions and conferences hosted by the U.S. Army, Pitney Bowes and U.S. Postal Service. They used knowledge from these courses, and information from the Centers for Disease Control and Prevention, to make mailroom operation safer. Special provisions were made to isolate and process mail addressed to senior Air Force offices in the Pentagon that could be potential terrorist targets.

When anthrax was found at the Brentwood USPS distribution facility – which is the servicing post office for the Pentagon and Bolling AFB – immediate action was taken to control mail flow, and to contact medical professionals for conducting mailroom testing and personnel evaluation.

Customers are provided updated information on anthrax risks, best methods for handling mail, and USPS mail bulletins. Town hall meetings, base newspaper articles and daily information notices on the base television channel help educate the base populace and keep them informed. The anthrax situation affects all Bolling housing residents, because all our mail is protected as “gov-

ernment official” and must be sanitized before delivery.

In early 2002, we hope to install the IONSCAN 400B scanning device, which will detect and identify trace amounts of drugs and explosives. The system has been successfully used in correctional facilities, airport security checkpoints, customs inspection and site security areas, drug interdiction missions and forensic operations.

We honor all the men and women assigned to the 11th Communications Squadron’s mail operation, who have joined the front line of defense in our nation’s war on terrorism.



**Airman Nicholas Grossman (left) and Airman 1st Class Jazzreal Richardson meter mail.**



**Airman 1st Class Jazzreal Richardson meters outgoing mail.**



**Airmen 1st Class Scott Molnar and Roland Jones sort mail from their daily distribution run on Bolling AFB, D.C.**



**Airman Nicholas Grossman secures distribution loading equipment on the BITC vehicle.**

# ACC postal services combat America's bio-terrorism threat



*Photo by Tech. Sgt. Robert Jackson*

**Airman 1st Class Stephanie Robinson and Airman 1st Class Yashika Harvey, 83rd Communications**

**Squadron, Langley AFB, Va., open Air Combat Command incoming mail.**

**By Capt. Daniel Leos**

*ACC Postal Services Flight Commander  
83rd Communications Squadron  
Langley AFB, Va.*

The tragic and shocking events of Sept. 11 changed our lives forever. As our military answered the President's call to help protect our homeland against terrorism and to take the offensive in battling terrorism worldwide, a second offensive attack hit the United States. Bio-chemical terrorism, in the form of anthrax, was introduced into our mail system. Our greatest fears were realized at just how vulnerable we were to this threat, as several innocent lives were lost to these random vicious acts. While our civilian leadership was targeted initially, the question became who would be next. How would we protect civilians? How would we protect our postal workers? As we sorted through these questions, a real possibility of threats to our nation's military was in the balance as well. Reacting logically and quickly, our military postal operations transitioned from

force build-up to support Operation Enduring Freedom, to defense of the homeland against this new terrorist threat. Air Combat Command postal services, from the 83rd Communications Squadron, at Langley AFB, partnered with the legal, medical, security forces, public affairs and civil engineering communities to develop a course of action against all dangerous mail. With force protection as the number one priority, these subject experts identified key approaches to dealing with dangerous mail: education, identification, protection and isolation.

The first challenge was the information war on anthrax. As soon as CNN reported the first contamination case in Florida, e-mail traffic on the anthrax threat was overwhelming. The ACC Postal Services Flight had the daunting task of educating, and providing guidance and directives, to commanders at every level. The concern spread like wildfire, and it became of paramount importance to disseminate crucial and accurate information quickly. Hours were spent researching information from Web sites, bulletins and expert

sources, like the Center for Disease Control and Prevention, FBI advisories, Office of Personnel Management for Bio-terrorism and the U.S. Postal Service. Within 48 hours, the latest information was synthesized into a plan to educate the military community, train military postal handlers in procedures to identify the threat, protect our personnel, and isolate the threat for proper disposition.

As part of the plan, ACC postal services modified an existing suspicious mail handling procedures handbook and provided a comprehensive package of support material, including CDC definitions on anthrax; a USPS training video dealing with anthrax and bombs; letters and memorandums from Air Staff and DOD; and USPS charts and bulletins on current threats.

To protect our Air Force installations from dangerous mail, three lines of defense were put in place. First security forces and working dogs provided mail screening at all base entry control points. Then official mail managers and base postal employees screened mail for suspicious packages at the official mail center. Finally organizational unit mail handlers visually screened mail prior to opening. Air Staff and DOD purchased state-of-the-art IONSCAN detection sniffers for all Air Force military post offices. These scanners detect explosive devices in mail packages and were deployed at critical overseas locations before the holidays arrived.

Emergency calls started to appear with hoaxes and fears of suspicious packages. Critical facili-

ties were shut down and base operations were affected with delays due to quarantined facilities. Test results and comprehensive inspections took days, causing some installations critical downtime. ACC developed a plan to isolate all ACC official mail centers away from critical facilities. The plan prevented official mail from being sent directly to a facility. Mail was screened by trained professionals and opened at this "centralized" mail facility. Bioenvironmental engineers inspected mail facilities to determine risk factors, and recommended appropriate individual protection equipment and procedures for mail handlers. Members encountering a suspicious package or letter were instructed not to tamper with or open the package, and to immediately call 911 for professional assistance. ACC proactively provided guidance to all numbered air forces and wing commanders on these policies, with instructions for implementing the guidance. A page was developed on the ACC Web site for Air Force and DOD members to gather vital information on dealing with the threat of dangerous mail -- <https://wwwmil.acc.af.mil/anthrax/anthrax.htm>

Bio-chemical terrorism challenged America's postal system and put Air Force mail handlers in harm's way. ACC responded by quickly preparing more than 790 mail handlers at 72 ACC mail facilities to deal with the threat. These initiatives provided commanders the tools to protect their people and facilities, and keep mail flowing throughout the armed services.

**A staff sergeant waits out a force protection situation.**

*Photo by Staff Sgt. Lynitta Cotten*



# Edwards' BITS forms first line of defense

By **Master Sgt. Stefanie Doner**  
*Public Affairs Specialist*  
and **Cheryl Middleton**  
*Chief, Information Management*  
*Air Force Flight Test Center*  
*Edwards AFB, Calif.*

With the heightened security that resulted from the Sept. 11 terrorist attacks and the introduction of biological agents into the U.S. Postal Service system, increased attention has been given to safety and security of military mail. In response to the threat, Edwards' base information transfer system, contracted to Superior Services, and members of the Air Force Flight Test Center's Information Technology directorate, have formed the first line of defense for letters and packages received by the base. It's a role they're well trained to perform.

Prior to the attacks, the base received 180,000 to 200,000 pieces of mail and 1,200-1,300 packages monthly. Since that time, the number of packages has increased significantly to about 2,500 a day, or 75,000 a month. All commercial carrier and USPS deliveries go to the base information transfer center. Packages are checked for potential explosive and biological threats on a 6-by-15-foot X-ray machine with a 40-by-40-inch opening. The machine works in the same manner as those commonly used for airport security screening. After contents are viewed and checked, packages are reloaded onto the carrier's truck and delivered.

"All of our people receive annual training, both from the U.S. Postal Service and Edwards' own explosive ordnance disposal experts," said Steve White, BITS manager. "We stay current by taking the initiative to look for the latest information on potential threats."

According to White, the heightened security measures have increased their workload, but they get a lot of help from base leadership and security agents.

"It's a real team effort," White said. "We're one of the first bases to purchase an X-ray machine for BITS. The office of special investigations detachment here sends us all the information they can to help us keep abreast of potential threats, and 95th Security Forces Squadron has been simply outstanding with their support."

White pointed out the 95th SFS and 95th Medical Group provided gloves for BITS employees, for



*Photo by Tech. Sgt. Christopher Ball, AFFTC/PA*  
**Senior Airman Edric Aselin, Air Force Flight Test Center Information Technology directorate, unloads parcels from BITC X-ray machine while Steve White, BITC manager, monitors the contents on the video screens.**

added mail handling protection until they got their own. He also praised security forces for rapid response to emergency calls to deal with suspicious mail.

White said the attitude of his workers is positive. "Of course they're concerned about the threat, but they know this is the focal point for all incoming mail and they have an important job to do. They've trained in all the scenarios for handling suspicious mail and they know what to do. They're very concerned about the safety of Edwards people, and they've shifted into a high gear that is simply indescribable."

Another important job is educating BITS customers by explaining potential threats and providing them as much information as possible. Organizational mail handlers were given posters detailing what to look for and how to report a suspicious package.

Customers are educated to be alert, and even if a suspicious letter or package doesn't fit the standard description for a threat, they're welcome to take it to BITS to go through the X-ray machine.

Contractors work a 7-day week to ward off potentially dangerous mail, ensuring base personnel can continue to fulfill their mission.

## MAIL

From Page 5

facility which in-turn performs an initial sort of the mail and sends the military mail to one of more than 200 processing and distribution centers. The center serves many post offices in a geographical region and dispatches military mail to one of eight USPS operated international service centers. The ISC sorts the mail by ZIP code (APO number), places the mail in pouches, and dispatches it to a multitude of foreign flag and U.S. commercial air carriers that deliver the mail to its overseas destination, where it will enter the military postal system. Depending on point of mailing and destination, the mail will be on an airplane four to six days after mailing, and will be delivered seven to nine days from the postmark. The accompanying illustration provides a thumbnail sketch of the postal network.

The ISCs use more than 60 airlines to dispatch military mail to more than 100 locations overseas daily. The overseas location could be an aerial mail terminal (military version of an ISC), or a geographically separated APO that dispatches and receives mail directly to and from the nearest airport.

Now let's say your Aunt Jenny or Uncle Joe want to save a couple of dollars, and you don't need those new socks that fast. They decide to send you

the package at the parcel post or 4th class rate. This package takes a slightly different route to get to you. Although postage is a little cheaper, the seven to nine day transit time expands to 30-35 days. This is because the parcel will travel from the P&DC to either Newark, N.J., or San Francisco to be placed on a ship to the overseas consolidation point, where it will be trucked to the destination.

MPS is a complex network of air and surface routes. Mail moves between overseas locations on more than 2,000 air segments daily. One benefit of MPS is mail doesn't travel from the overseas area to CONUS by ship – all mail flies. Once it reaches CONUS, parcel post and 4th class mail reach the destination by truck. Another benefit of MPS is mail is dispatched to the CONUS ISC closest to the end destination, saving processing steps and time, and ultimately speeding delivery of that package to the correct destination.

The Air Force commits about \$50 million annually to pay for transporting items folks like Uncle Joe and Aunt Jenny exchange with loved ones overseas. If you're still wondering what makes that airman smile behind the counter of your local APO, it's because they know the impact their job has on morale and the mission. Nothing makes them happier than to provide world-class service, ensuring Uncle Joe and Aunt Jenny's package arrives in your mailbox.

---

## DETECTION

From Page 7

after we began the research phase," he added. "The speed with which we are able to identify, acquire and field these systems was aided by the fact that it's commercial off-the shelf equipment," the chief explained.

Chief Small said training to support the systems was worked in parallel with the acquisition process. "As you might expect, we worked hard to lead turn the training for these systems," he said. "We were able to rapidly develop and disseminate training and certification standards by partnering subject matter experts at USAFE's Air Postal

Squadron, with training specialists from Air Education and Training Command's 81st Training Support Squadron Qualification Flight," Chief Small added. He said training to support the system is less costly and complex than for X-ray and other types of explosive detection equipment. "Many systems we researched required substantially longer and more in-depth training," the chief remarked. "Our goal is to provide a system that not only affords greater security during times of increased force protection conditions or directed threats, but also enables people to focus on their core mission of moving the mail. This equipment will enable postal special-

ists to be just that, postal specialists, and not experts at deciphering things like X-ray images, because the system performs the analysis and issues a warning," Chief Small said.

The Air Force has more than 700 postal specialists serving in 123 air post offices, 13 aerial mail terminals and mail control activities, and five joint military postal activities around the globe supporting the military postal service. In a typical year they serve nearly one million patrons, including 200,000 on deployment, and receive, process and dispatch more than 200 million pounds of mail. (*Courtesy Air Force Postal Policy Element*)

# PACAF postal service protects your mail

By Senior Master Sgt. John V. Czumalowski  
*Superintendent, Postal Plans and Programs*  
*HQ Pacific Air Forces*  
*Hickam AFB, Hawaii*

Can you safely open your mail? Pacific Air Forces' postal personnel are doing their best to ensure their customers answer with a resounding yes. After anthrax contamination was discovered at U.S. Postal Service facilities in October, PACAF personnel teamed with the Military Postal Service Agency and other organizations to enhance mail security and force protection measures for postal clerks handling potentially hazardous mail. Procedural changes were implemented throughout MPS.

At DOD level, MPSA coordinated with USPS to ensure all facilities responsible for processing military mail were tested for anthrax contamination. Included was the International Service Center in San Francisco, which processes virtually all letter mail destined to military post offices in the Pacific theater. The facility was screened and certified to be anthrax-free in mid November. MPSA also initiated deployment of scanning systems for all DOD post offices, and provide user training to detect mail bombs, narcotics and other contraband.

Headquarters directorates held a special meeting of the PACAF Force Protection Working Group – including postal, security forces, surgeon general, and civil engineering personnel – to attack the anthrax contamination issue on all fronts. Chief among the products of this meeting was development of a Protective Support to PACAF Postal Workers Plan, with protection focused in four areas: assessing the workplace environment, personal protective equipment, incident management and medical support.

To assess the workplace at local level, a team comprised of civil engineer, security forces, and medical personnel is responsible for risk analysis, threat assessment and environmental sampling. In regard to personal protective equipment, PACAF Air Postal Squadron personnel took the initiative to procure disposable protective gloves and respirators through MPSA for a mail processing work force of more than 300 military, U.S. civilian, and foreign national personnel. Local bioenvironmental engineers are responsible for coordi-



**Staff Sgt. Portiah Leacock (left) and Staff Sgt. Stacy Servillon sort mail at the Yokota AB, Japan, aerial mail terminal.**

nating with postal personnel to determine appropriate levels of personal protective equipment, and for fit-testing and training on proper wear and use of respirators. In addition to being regarded as a possible crime scene, all anthrax contaminations are treated as hazardous materials incidents, with local medical, fire and explosive ordnance disposal personnel following standardized PACAF procedures. Postal personnel are responsible for reporting any damage to mail or USPS effects. Medical treatment of mail handling personnel at suspected anthrax contamination sites follows guidelines established by the Centers for Disease Control or the Air Force Medical Operations Agency, depending on risk of exposure.

At local level, several PACAF postal activities enacted procedures to meet or exceed CDC and AFMOA guidelines. To isolate and reduce num-



**A deployed postal worker sorts mail at Prince Sultan AB, Saudi Arabia.**

bers of personnel exposed to the mail, the 374th Communications Squadron APO at Yokota AB, Japan, temporarily moved its mail processing function to an isolated area of the Yokota Aerial Mail Terminal operated by Yokota's Det. 2, PACAF Air Postal Squadron. The isolated area and equipment are wiped down and cleaned with a chlorine bleach solution daily. Personnel also refrain from eating or drinking in mail processing areas. All this is done at PACAF's busiest postal activity that processes more than 18.1 million pounds of mail annually. At Misawa AB, Japan, 35th Communications Squadron postal personnel established and marked off zones throughout the post office to assist in identifying and limiting exposure should hazardous materials be detected. The Seoul AMT in Korea fluoroscopes all mail entering the country, and in conjunction with a suspected exposure, Army and Air Force post offices in Korea were thoroughly tested for anthrax as a precautionary mea-

sure, with negative results.

Enhanced security isn't limited to personal mail. Hickam's 15th Air Base Wing officials trained activity distribution office personnel on handling suspect mail and protective measures. Base information transfer center personnel at the 3rd CS at Elmendorf AFB, Alaska, are procuring industrial strength, high-efficiency particulate air vacuum cleaners to effectively clean mail processing areas. Similar measures are in place at all PACAF official mail centers.

During the 2001 holiday mail season, PACAF postal representatives encouraged postal customers to enjoy the same seasonal mailing traditions as in past years, but emphasized the need for strict adherence to military mail requirements. Whether mail is retrieved from a personal receptacle or delivered to the office, PACAF postal customers can rest assured all available protective measures are being employed to safeguard their mail.

# Reservists augment active-duty postal units

By Chief Master Sgt.  
**Dave Stantz**  
*Directorate of  
Communications and  
Information  
HQ Air Force Reserve  
Command  
Robins AFB, Ga.*

Since 1989, members of the Air Force Reserve, now Air Force Reserve Command, have volunteered more than 12,000 mandays of support to Air Force postal units worldwide during the annual Christmas rush. While helping to deliver mail, they've also received valuable hands-on training. In all, more than 850 reservists have served one or more two-week active duty tours in Air Force post offices, aerial mail terminals, and mail control activities at 34 locations throughout Pacific Air Forces and U.S. Air Forces in Europe.

Nearly all AFRC wings are tasked to augment APOs and AMTs during wartime or other contingencies, with unit type codes 6KDB3 and/or 6KDB4. However, since APOs and AMTs are not located at stateside bases, Air Force reservists assigned to those UTCs can't receive adequate training at home station.

In fall of 1989, while AFRC was seeking solutions to their training problem, the USAFE Air Postal Squadron (then 7025th AIRPS) was looking for fixes for an anticipated manpower shortage during the upcoming Christ-

mas mailing season. The commander of the 7025th AIRPS at that time had arrived only a few months earlier from an assignment at HQ AFRC and suggested asking them for help.

The result was a mutually beneficial arrangement, with reservists receiving on-the-job training and experience, while the APO or AMT, as a by-product of training, received a manpower boost at a critical time. Participation during that first year was limited to three locations in USAFE. PACAF was included the following year, and since then the number of locations expanded to 34.

When Air Expeditionary Force scheduling began, AFRC was tasked to provide postal augmentees throughout the year in two-week active duty rotations for the APOs at Aviano AB, Italy, and Incirlik AB, Turkey. Taskings are scheduled to increase in the upcoming AEF cycle. These much higher priority AEF requirements raised concerns that the Christmas-time postal augmentation training program might be competing with AEF taskings for the limited availability of reservists.

Even though AFRC continues to provide this valuable service, world events since Sept. 11 led the command to suspend the 2001 Christmas program. We hope to be back "out there" this year.

# Texas squadron supports Operation Noble Eagle

By Capt. **Walter J. Brown**  
*221st Combat  
Communications Squadron  
Texas Air National Guard  
Garland, Texas*

The 221st Combat Communications Squadron, Texas Air National Guard, put their monthly training efforts to the test in September by performing a real-world mission.

On short notice, the 221st deployed a 19-member team with tactical communications resources to Camp Mabry, in Austin, home to Texas National Guard Headquarters, in support of Operation Noble Eagle. The team was tasked to provide tactical communications satellite access for the headquarters command staff's information operations cell, to give them secure and non-secure voice and data capability.

The squadron activated a tactical satellite terminal, a deployable local area network and a switch in support of this mission in record time. The system enhanced the base communications system, provided point-to-point voice, commercial and DSN secure and non-secure voice, and gave secure and non-secure access to Internet-based communications. The mission allowed the 221st CBCS to demonstrate its ability to quickly and reliably deploy and install these tactical communications assets. The 221st reaffirmed its readiness to provide communications services anytime and anywhere.



# Thule heightens mail handling security

By Kathy Kite

*Plans, Policy*

*and Resources Division*

*Directorate of Communications  
and Information*

*HQ Air Force Space Command*

*Peterson AFB, Colo.*

Even if the threat seems far away, residents of the close-knit community of Thule AB, Greenland, rely on their postal operations to take mail handling seriously.

Located 695 miles north of the Arctic Circle at the Air Force's northern-most base – where it's cold, dark and windy – the Thule postal team recognizes customer concerns and has responded to the challenge.

Since identification of anthrax in U.S. Postal Service offices in October, Air Force Space Command has worked diligently to equip their mail handlers to process mail safely. In concert with guidelines from the Centers for Disease Control and Prevention, Federal Bureau of Investigation, and the U.S. Postal Service, new checklists were developed to help identify suspicious packages and letters.

Partnerships were formed throughout the command between medical groups, civil engineers, security forces, Offices of Special Investigation, and command sections to conduct an aggressive and informative education and awareness campaign at many locations such as Thule.

Since receiving mail is important to the quality of life of Thule airmen, base mail handlers – who are the first line of defense for the base populace – have stepped up safety procedures to mitigate risk of exposure to biological and chemical hazards.

Under new safety procedures for incoming mail, Thule mail handlers wear gloves and have the option to wear masks. Following a suspicious mail threat checklist, they first conduct a visual assessment of each item, looking for things like stains, watermarks, restrictive markings, excessive wrap-



*Photo by Tech. Sergeant Howard Hollister*

**Senior Airman Hilda Haftmann, mail handler at the Thule post office, screens incoming mail for suspicious content.**

ping material, odors, oddly shaped items, excessive or no postage, incorrect or inaccurate titles, no return address, and crystallization on wrappers.

When it's determined an item doesn't meet suspicious mail criteria, it's deemed deliverable to the intended recipient. But stepped-up precautions don't end there. Thule mail handlers have been educating the base population to be better informed and equipped to deal with the anthrax threat and ways to identify suspicious mail. Additionally, Thule will be receiving a scanner to help detect drugs and explosive hazards this year.

Along with their partners in security forces and the bioenvironmental community, Thule postal workers are committed to making mail handling as safe as possible. As in postal operations throughout the nation, Thule is no exception: they take this responsibility seriously.

Extraordinary times have made us more aware of the work of these relatively inconspicuous individuals, who normally go about their work quietly, but now more than ever, are being recognized for their efforts to protect each of us from potential mail threats. Our mail handlers are our source of confidence that our mail is safe – and we're most appreciative of their significant contributions to assuring our readiness to perform our missions.

# Neither rain, nor snow, nor bombs, nor anthrax ...

By Senior Master Sgt. Salvador Orozpe  
*Systems Operations Branch*  
HQ Air Education and Training Command  
*Randolph AFB, Texas*

Remember the importance of mail call when you entered the Air Force? Thrust into the new and challenging environments of basic military training and technical school, your main contact with what was familiar may have been through the U.S. Postal Service. Unfortunately, the anticipated pleasure of opening a mail package wasn't always warranted, as we realized in July when one of our people was severely injured opening a parcel bomb. In addition to that threat, we must now deal with the potential for bio-terrorism.

The previously simple act of opening an envelope may invoke suspicion, if not fear, requiring management to respond to questions about the safety and security of our most valuable resource, our people. Air Education and Training Command has taken dramatic action to keep its bases, and postal folks on the front lines, informed and ready to handle any contingency. In times of crisis, people are desperate for information from credible authority – lacking that, they tend to listen to rumors.

Here are some facts on what AETC is doing.

- HQ AETC continues to forward all information from HQ Air Force, Department of Defense, Federal Bureau of Investigation, Centers for Disease Control and Prevention, USPS, and major command units to field organizations.

- Lackland AFB held a base-wide briefing for personnel who handle mail.

- Postal personnel placed FBI and USPS posters, "What Constitutes a Suspicious Letter or Parcel," in their facilities and briefed personnel on proper procedures.

- All mailrooms were assessed by local bioenvironmental engineering personnel to determine potential health risks based on the CDC health advisory notice.

- Seven IONSCAN model B scanners have been ordered for delivery in January through March. They can detect explosives such as RDX, TNT or Semtex.

- Communications squadron commanders are identifying possible alternate postal operations sites if anthrax is found in their facilities.

- Web sites were created to keep personnel informed on the latest information.

- Units have obtained personal protective equipment, such as gloves, for use by mail handlers. Personnel were briefed on the proper wear of PPE, and safety concerns regarding wearing gloves around equipment.

- Bases are completing the Military Postal Service Agency requirement for location information. Knowing which USPS facilities process our mail is crucial, in case an incident is reported and quick reaction is required.

AETC is working to maintain confidence in our mail system and keep our personnel informed and protected. The mail will get through!

**Airman 1st Class Jazzreal Richardson (left) and Airman Nicholas Grossman, 11th Communications Squadron, Bolling AFB, D.C., meter outgoing mail.**

*Photo by Staff Sgt. Brian M. Boisvert, 11th CS*



# System availability in war represents ancient requirement, modern challenge

By David L. Taylor

Research Analyst, Analytic Services Inc.  
and Lt. Col. Donna G. Schutzius  
Chief, Information Assurance Policy Branch  
Air Force Deputy Chief of Staff  
For Communications and Information  
Washington

Careful study of political and military history helps ensure we don't repeat mistakes. Study of military doctrine keeps us grounded in how and why our doctrine and tactics evolved. The lessons of military history sometimes revive or reinforce good ideas from the distant past. Communications and information system availability is a prime example. More than 2,500 years ago, Sun Tzu referred to one of the earliest known military doctrine documents. The ancient Chinese "Book of Military Administration" directed, "As the voice cannot be heard in battle, drums and bells are used. As troops cannot see each other clearly in battle, flags and banners are used." This doctrine specified use of amplified visual and audio signals for command and control of military forces. Employment of these systems had two main purposes: command, or communication of orders from the commander to his deployed

forces; and control, or maintaining unity of effort among his forces. Sun Tzu advocated the unifying effect (control) of this C2 system as a distinct advantage in battle saying, "Now gongs and drums, banners and flags are used to focus the attention of the troops. When troops can be thus united, the brave cannot advance alone, nor can the cowardly withdraw." Finally Sun Tzu strongly urged military commanders to provide maximum *availability* of these systems when he said, "In night fighting use many torches and drums, in day fighting many banners and flags in order to influence the sight and hearing of our troops."

This type of basic visual and audio C2 system remained relatively standard, with minor variations through the ages, in many worldwide cultures, until World War I. The system worked well, but was limited to mostly open field or surface ship warfare. It also required command elements to be either in or very near the field of battle to monitor progress and issue commands. However, open field warfare became increasingly obsolete as weapon systems became more powerful, and signal and information communications capabilities greatly improved with the advent of telegraph, telephone

See **SYSTEM AVAILABILITY** Page 31



The RQ-1 Predator is a medium-altitude, long-endurance unmanned aerial vehicle system. The Predator is not just an aircraft, but a fully operational system consisting

of four air vehicles (with sensors), a ground control station, a Predator primary satellite link communications suite and 55 people.

# Information Assurance Campaign 2002 Theme Schedule

January  
Contingency Planning  
for the Global Strike Task Force  
AFCA

February  
Portable Electronic Devices  
AFPCA

March  
Securing Air Force Operations  
ACC and AIA

April  
Remanence Security  
Sanitization and Destruction  
AMC and AFSOC

May  
E-mail  
AETC and AFWA

June  
Vulnerabilities and Incidents  
AFOSI and AFIWC (AFCERT)

July  
The Air Force  
Enterprise Network  
AFMC and AFNOC (SSG)

August  
Public Key Infrastructure  
AFRC and ANG

September  
Viruses  
USAFE

October  
No IA articles  
(Almanac issue)

November  
October's theme  
User Responsibilities  
AFSPC and USAFA

December  
Web Security  
PACAF  
IA Campaign in Review  
AF/SC

# Protecting critical infrastructures key to IA

By **Jim Garamone**  
*American Forces Press Service*  
Arlington, Va.

**E**ven before Sept. 11, DOD recognized the importance of protecting critical infrastructures.

For more than two years, experts in the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence have been working to identify DOD's critical assets and their associated supporting infrastructures, to develop policy on their protection, and to game how the department would work if a node in these infrastructures were destroyed.

As director of the Critical Infrastructure Protection Office, Tom Bozek leads a small staff that's putting in place policy framework to protect critical infrastructure.

The military has long known certain physical or cyber capabilities are essential to protect the nation. They're also essential to help the military accomplish its missions. Measures can be as mundane as physically protecting a facility or installation, to ensuring satellite communications continue uninterrupted. The office studies the big picture and applies lessons to specific fixes.

"We want to learn the lessons once and implement the solutions many times," Bozek said.

Bozek's office works with the warfighting commands to determine what capabilities are critical to their missions. Then the office works with the service or agency that "owns" the asset to ensure the capability is protected or that procedures are established so the mission continues in the event of a breakdown.

It's a big job. "We're trying to understand what assets are critical to military mission success," Bozek said. The office concentrates on these critical infrastructures: transportation, logistics, financial services, public works, health affairs, personnel, defense information, space, and intelligence, surveillance and reconnaissance.

Bozek said the picture is complicated because there are many interrelationships between the various infrastructures. "We know there are interrelationships among the assets in these infrastructures," he said. An asset failure in one infrastructure may have an adverse cascading effect on assets in many other infrastructures.

Once the group defines interdependencies, it isolates single points of failure that could cause mission failures.

The group has built on the Year 2000 computer bug effort. "We're taking advantage of Y2K experiences. That's a good example of the interdependencies," Bozek said. "You have a variety of information systems that are connected. They pass data to each other through this network. The same is true on physical infrastructures – transportation, logistics, financial services and so on. So, we find the same principles apply to these infrastructures that we learned in Y2K."

The office calls on many different agencies for help. Bozek relies on the Navy's Joint Program Office for Special Technology Countermeasures as overall technical agent. He also calls on the Defense Threat Reduction Agency for balanced survivability assessments.

In addition, the office works closely with the Homeland Security Division of the Joint Staff, and with all the combat commands, services and combat support agencies. The office also works with the FBI and the National Infrastructure Protection Center.

The Sept. 11 events underscored the military need for redundant facilities and partnerships with private industries. The New York attacks, for example, illustrated the robustness of U.S. telecommunications facilities. Private telecommunications companies – also used by DOD – reconstituted financial communications networks fairly quickly.

But the attacks illustrated how much the military relies on private firms for infrastructure support. "We're dependent on our private sector partners," Bozek said. "Our telecom is over private lines, most bases take power from private sources. Private shipping lines augment our sealift and airlift.

"We're developing even closer relationships with our private partners to identify potential vulnerabilities and to get better."

In light of asymmetrical threats the U.S. military faces, the mission given Bozek's office is never-ending.

"Critical infrastructure protection has a defensive focus – offense almost always has the advantage," he said. "Adversaries are always going to try newer creative ways to overcome our defenses. Everyone needs to be vigilant."

# Back up electronic files

By Lynne Kuykendall  
Information Assurance Office  
Air Force Communications Agency  
Scott AFB, Ill.

It's essential for information systems users to safeguard important computer files by regularly backing them up. This practice minimizes data loss if your hard drive crashes or is infected by a virus. Another good practice is having a set of your back-up files off-site, in case of fire or flood. Storing back-ups in a metal cabinet or safe provides greater protection from fire and water damage. Label back-ups to indicate sensitivity level of the information. To prevent erasures, keep backups on diskettes away from magnetic sources (i.e., radios and telephones). Taking time to follow these preventive steps will minimize potential for losing electronic files.

The following instructions are provided on a couple of ways to back up your computer files: how to archive important e-mails, and how to burn or copy files to a CD. If these instructions don't work on your system, check with your information systems security officer for guidance.

## Archiving e-mail messages

- \* In Outlook, click on File
- \* Select Archive



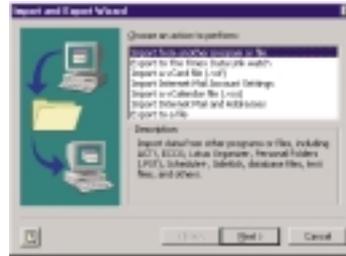
☞ Ensure you have selected "Archive this folder and all subfolders."

☞ Select a date at least 3 months prior to the current date in "Archive items older than."

\* Ensure you are archiving to your P:\ drive and the extension is .pst (or any other drive/disk/CD). Click OK.

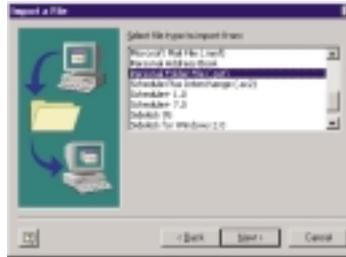
To retrieve these files do the following:

- \* Click on File
- \* Select Import and Export
- \* Import and Export Wizard screen will appear



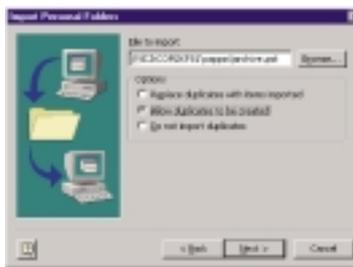
☞ Select "Import from another program or file" (should be the first choice)

- \* Click on Next
- \* Import a File screen appears



☞ Select Personal Folder File (.pst)

- \* Click on Next
- \* Import Personal Folders screen appears



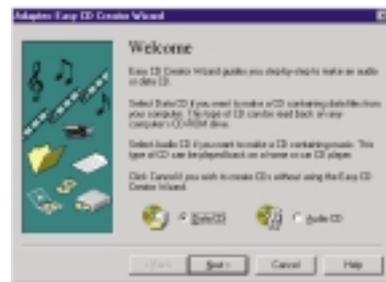
☞ Click on Browse and go to the P:\ and find the .pst file. (or any other drive/disk/CD).

☞ Select "Allow duplicates to be created"

- \* Click on Next
- Now it should start pulling those files back

## Copying files to a CD

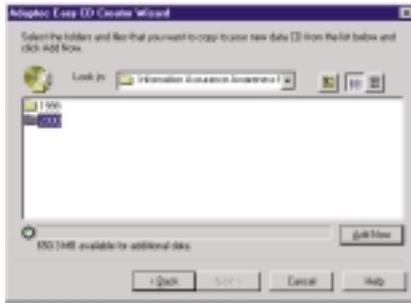
- \* Select Start
- \* Programs
- \* Select Adaptec Easy CD Creator
- \* Easy CD Creator
- \* Next
- \* Insert writeable CD
- \* Next



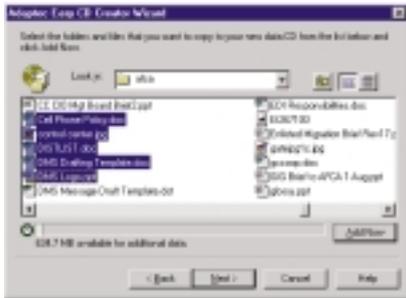
Ensure Data CD radio button is highlighted

- \* Click on Next
- \* OK

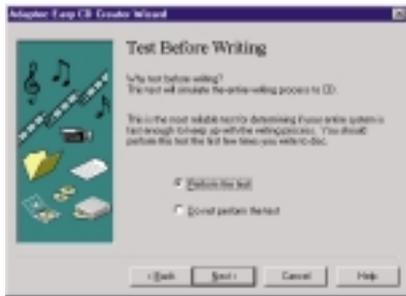
- \* Adaptec Easy CD Creator Wizard Appears
- \* Select those folders and files that you want to copy



- \* Once you have selected your folders—click Add Now



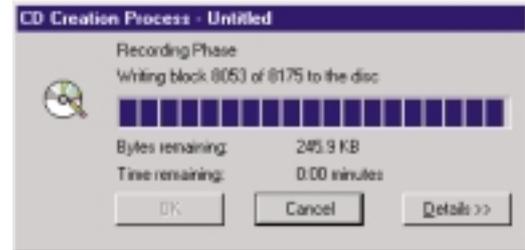
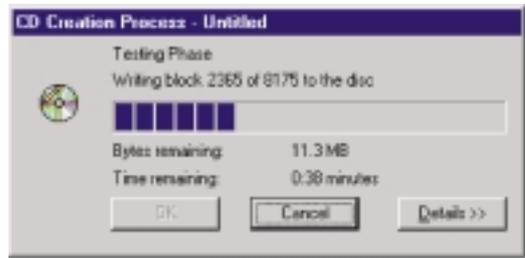
- \* Once you have selected your files—click Add Now
- \* Next



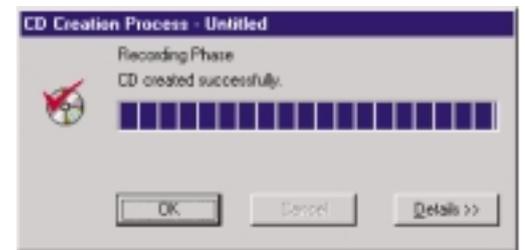
- \* Ensure you Perform the test
- \* This will ensure the CD is not damaged
- \* Next



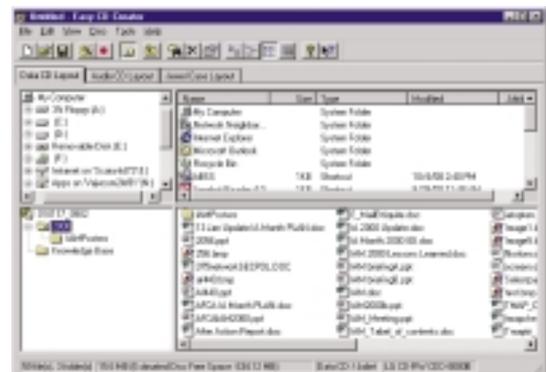
- \* Finish



- \* CD Creation Process starts
- \* Upon completion of copying, the CD will pop out and you'll see the following screen:



- \* OK—You have successfully copied your files to your CD



- \* You should see all the folders and files you copied in the lower panel

# *How important is your data?*

**By Cynthia M. Crowe**  
*Systems Security Analyst*  
*Air Force Communications Agency*  
*Scott AFB, Ill.*

You're back to work after the holidays and you turn on your computer. While you're waiting for it to boot up, you grab your morning cup of coffee. You had a great time on your days off and nothing can spoil your good mood today. Well, almost nothing. You reach over and recheck the power button on the monitor. You think, "Why isn't this darn computer coming up?" You know that when you left the office to go on leave, you weren't having any problems with your computer. You check the power cords on the computer and monitor – they're still plugged in. After you've exhausted all the obvious possibilities, you resort to calling the Help Desk, which later sends someone to check out the situation. That's when you hear the dreaded, "I'm sorry to tell you, but your hard drive has crashed. We're going to have to take your computer with us. Just reload your backup data on the new computer we bring you, then you'll be up and running in no time." You shake your head in disbelief, since you never took the time to back up your data.

Hopefully, this scenario has never happened to you. But statistically, some of us don't get serious about backing up our data until it's too late. We're always busy and in a hurry to do everything – that is, everything except back up our data. Unfortunately, we may not realize how important our data is, until we don't have it.

System administrators are responsible for backing up data stored on servers. However, if the data is on your computer's hard drive, no one else is going to back it up for you. Depending on the importance of your data, it may be advisable to back it up monthly, weekly or even daily.

How much of your data can you afford to lose? If the answer is none, then YOU need to ensure you back it up on a regular basis.

Gone are the days of backing up data on floppy disk. With today's technology, it's more practical to use a ZIP disk or compact disk. With the relatively low price of CDs today, they make cheap storage media for larger files.

Yes, it takes time out of your work day to back up your files, but think about it: How long would it take you to recover if tomorrow everything was gone from your hard drive?



# Plan for the worst

## ‘Things that go bump in the night’

By Dr. Timothy Mucklow  
Information Technology Directorate  
Air Force Communications Agency  
Scott AFB, Ill.

“From ghosties and ghoulies and long-legged beasties and things that go bump in the night, may the Good Lord deliver us.” So went a prayer in the 1500s. Unfortunately, because of events in recent months, we can no longer or so easily dismiss the seemingly remote prospect of things going bump in the night. Within easy memory, the Air Force has lost information technology resources and information to acts of God – including fire, flood, storm and volcanic eruption – and to willful depredations of man, manifested by terrorist attacks, malicious logic, theft, hacking, and well-intentioned “Forrest Gumps” who so willingly lend an inept hand. Only the ravages of plague seem to be absent, and even that may no longer be a hollow threat.

What was once Murphy’s Theorem is now Murphy’s Law. And if our systems are to provide mission support for which they were intended, we must be prepared. The “DOD Information Technology Security Certification and Accreditation Process (DITSCAP),” [DOD 8510.1-M], Appendix L, requires that **all** DOD systems have contingency plans ... just in case something goes bump in the night. The efficacy of these plans, however, is entirely reliant on thoroughness of the accreditation process, and all too often is given short shrift when compiling a system security authorization agreement. In many cases, it hasn’t been addressed at all. As the late Admiral Daniel V. Gallery once noted, “In war, defeat is the inevitable consequence for the poorly prepared.” Thus our failure to have adequate back-up plans for our systems dooms us to failure.

Before the unthinkable happens again, we need to review our contingency plans. If none exists, now is the time to create one. A good contingency plan is based on realistic assessment of requirements, not wants. It identifies resources to use if part or all of your primary system is lost. Such a plan also includes well-defined courses of action needed to restore minimal mission capability.

When manual workarounds are envisioned, you need to document resources, methodologies and procedures. If contingency plans include sharing equipment or facilities of another organization, formal agreements need to be in place. When plans call for off-site storage of media or equipment, remember the location must be both secure and geographically-separated, not just down the hall or in the basement.

As with the rest of the SSAA package, the contingency plan’s currency needs to be maintained. Just as importantly, the plan must be periodically exercised. Though a plan may look splendid tucked away in a file cabinet, it may not necessarily function as designed. The only way to ensure its value is to test it in a realistic scenario. The results may offer some surprises.

Fortunately an effective contingency plan need not prove elusive. Many models abound. You can research the SSAAs of comparable systems within your own organization or on base – in other words, rip off a copy and use it as a baseline. To assist you in developing or honing plans, a number of official policy and guidance sources are available online:

- “DITSCAP, Department of Defense Information Technology Security Certification and Accreditation Process,” (DOD 8510.1-M) – this is a MUST.
- NIST Special Publication 800-12, “An Introduction to Computer Security: The NIST Handbook” – at nearly 300 pages, it’s a good general reference document, and a useful doorstop when you’re finished with it.
- FIPS Pub 87, “Guidelines for ADP Contingency Planning,” 1981 – slightly dated, but still worth consulting.
- AFRP 10-24, “Air Force Critical Infrastructure Protection” – not of much value to the bolt turner, but provides direction for higher levels.

Additionally, a series of National Security Telecommunications and Information Systems Security Instructions provides insights on what you, as an IT professional, need to know about contingency planning:

See **PLAN** Page 31

## OPSEC: Now it's personal!

# 'D\*I\*C\*E\* Man' shares thoughts on Sept. 11

By Ray Semko

*Interagency Operations Security Support Staff  
Greenbelt, Md.*

Do you remember what you were doing Sept. 10? It was just another Monday, and everyone went to work giving little thought to existing threats to our way of life. While Sept. 11 started the same way, unfortunately it didn't end that way. Instead it joined the ranks of dates such as Dec. 7, 1941, and Nov. 22, 1963, on which events occurred that had a profound effect on every living American and those about to be born. From the moment of the first terrorist attack on the World Trade Center, America was irrevocably changed. Belief in the invulnerability of our country disappeared, with little hope of returning anytime soon. So where do we go from here? For those of us in the security realm, our job should be less difficult in one regard: We no longer have to convince people of the threat.

Our mission now is to educate people that our society's openness, and our willingness to share every minute piece of information with the world, has proved to be of great value to our adversaries – in this case, terrorists who pulled off what was, in reality, a low-tech operation. They used computer systems to their advantage, because we try to make everything easy in this country. The terrorists knew every hijacked flight was going to be light, because that information is readily available on the Web. They didn't have to spend money on sophisticated equipment, since they had access to computers in our public libraries to communicate with each other, coordinate their plans, do research, make new contacts, and carry out other activities.

When the terrorists needed identification cards, they looked for weak links: Americans who were willing to circumvent the system for a little money. In addition, they used our own commercial passenger planes against us. They capitalized on security vulnerabilities at airports, exploiting information that was readily available or easily observed. They noted our limitations, worked around strengths, and exhibited great patience in planning and carrying out their operations. They used operations security to avoid detection.

A standard practice for us in evaluating circumstances surrounding a crisis is to prepare lessons learned; unfortunately, these reports often go unread. This time, however, we *must* get serious and educate the defense community and the entire country to recognize indicators that should be reported. As the deaths of thousands of civilians within our borders has shown, our enemies aren't just targeting the military now – and the threat of more terrorist acts remains.

### **OPSEC is personal.**

Operations security has been considered by many to be a subset of traditional security. Many people believed if they weren't in the military, OPSEC didn't apply to them. With the attack on our homeland, our attitude toward the OPSEC process must change, because *now it's personal*. OPSEC now needs to be incorporated into every facet of our personal lives. While OPSEC focuses on protecting sensitive, but unclassified, critical information, we now know it's the very information the terrorists used against us.

OPSEC has always stressed awareness of indicators. In the past, Americans haven't felt the need to worry about revealing indicators or predictable behavior that could be of value to our enemies. They were lulled into a false sense of security. It's our job to educate and ingrain in everyone the real need for caution in every aspect of their lives. *On the whole, we don't have bad security in this country – what we have is a bad attitude toward security.* If we don't change Americans' attitude toward security, we'll continue to be as vulnerable tomorrow as we were on Sept. 11 – and we won't stand a chance of thwarting an adversary intent on doing deadly harm.

### **Meeting the challenge.**

The Interagency OPSEC Support Staff has long recognized the need to be proactive in addressing new threats to the country. Now everyone must practice OPSEC to protect themselves, their families, their mission and their nation. If you take care of yourself, you'll be able to protect your family. If you take care of your mission, you'll be able to protect the nation. While our adversaries have reveled in our grief and anticipation of our down-

See **PERSONAL** next page

## PERSONAL

*From previous page*

fall, we, and the rest of the world, have learned we're not invulnerable.

### **IOSS can help.**

The IOSS has products available on request to assist security offices in meeting the challenges we all face – and will send them to you promptly to help you make the most of promoting OPSEC education in your organization. This is essential as we retaliate for the events that occurred in New York City and Washington, D.C., since we have to be able to surprise the enemy like they surprised us. If we don't protect our sensitive, critical information, the surprise party will be a bust. The IOSS

is also developing new products to address future needs. We're reaching out to our customers and anyone that needs our assistance. Go to the Web page, check it often, and spread the word: Good OPSEC saves lives. (Article courtesy *The OPSEC Indicator – Special Edition, Fall 2001/Winter 2002* newsletter)

*(Editor's note: Ray Semko, a.k.a. "D\*I\*C\*E Man," has presented briefings on Defense Information to Counter Espionage, both in person and on video, to hundreds of thousands of individuals in the national defense community over the past 12 years. His presentation style is noted for leaving a lasting impression. For more information on D\*I\*C\*E Man and OPSEC, visit the IOSS Web page at <http://www.ioass.gov>.)*

---

## SYSTEM AVAILABILITY

*From Page 23*

and radio. Military application of these inventions enabled commanders to coordinate movement and employment of significantly larger combat forces capable of securing and occupying larger areas of land, sea and air. Modern capabilities – including development and employment of effective technological innovations – have permitted command structure and a significant amount of allocated combat forces to be located far from the theater or field of battle.

Although weapons and communications systems have evolved, the basic concept of protecting system availability has remained constant. System availability is simply keeping systems available to users. They

must work as efficiently as possible, and if attacked, they must be able to recover with minimum adverse mission impact. As a related historical analogy, military buglers from the past three centuries were normally protected from front-line operations or battle, to ensure their efficient and specialized bugle calls remained available to the commander. Simple, distinctive open-horn melodies (limited to only four notes with varied rhythm and articulation) signaled attack, retreat and many other commands for combat forces. The combat bugler's importance in battle made him a highly desirable target. Capturing or killing an enemy's bugler not only denied the opposing commander an important service, but potentially degraded combat efficiency and capability.

Protecting the bugler became one of the commander's top priorities, in order to ensure continued availability of communications.

As the Air Force's Information Assurance campaign continues into 2002, we must make warfighter operations our top priority. Today fighter and bomber pilots, as well as unmanned aerial vehicle controllers, comprise a significant portion of our combat front line. Real-time data fusion and air tasking orders have replaced ancient banners, flags, gongs, drums and bugles. Since our modern, high-tech communications systems have become increasingly important to warfighter success, each of us must help to ensure their continued availability by observing the policies and practices of Information Assurance.

---

## PLAN

*From Page 29*

\* NSTISSI No. 4011, "National Training Standard for Information Systems (INFOSEC) Professionals"

\* NSTISSI No. 4012, "National Training Standard for Designated Approving Authority"

\* NSTISSI No. 4013, "National Training Standard for Systems Administrators in Information

Systems Security (INFOSEC)"

\* NSTISSI No. 4014, "National Training Standard for Information Systems Security Officers (ISSO)"

\* NSTISSI No. 4015, "National Training Standard for System Certifiers"

As part of January's IA focus on contingency planning, let's all take a long, hard look at our contingency plans ... before something does go bump in the night.

# Theater deployable communications makes vital contribution to Operation Enduring Freedom

By Jim Binniker

*TDC Implementation Team Member  
HQ Air Combat Command  
Langley AFB, Va.*

Within hours of the Sept. 11 attacks on America, Air Force communications warriors began planning to support whatever response option the President would choose to exercise. A critical component of the Operation Enduring Freedom communications architecture is theater deployable communications. With modern intelligence, surveillance and reconnaissance assets like Predator and Global Hawk available to OEF commanders, fast, reliable communications is more important than ever – not only as a warfighting tool, but to help safeguard our deployed airmen who find themselves in harm's way. In the first real test of the Air Force's new communications system, TDC's performance has been superb.

TDC fields a deployed communications infrastructure based on modern, commercial off-the-shelf technology and is the communications mainstay of the Aerospace Expeditionary Force. With TDC, AEF lead wings in Air Combat Command, Pacific Air Forces, and U.S. Air Forces in Europe can provide expeditionary deployed comm and info services for a base population of up to 1,200 personnel. Air Mobility Command and Air Force Special Operations Command are equipped to establish similar base infrastructure, in addition to supporting their respective air mobility and special operations missions. Besides the AEF wings, TDC is being fielded to active duty and Air National Guard combat communications units to robust the AEF wings, which together will service more than 3,000 deployed personnel at each location. Because TDC is modular, communications can now be tailored to support specific mission needs, while reducing the need for scarce airlift resources. Now that AEF wings are equipped, we will focus on robusting combat communications units and the ground theater air control system. As TDC is fielded to these units, we can retire many pieces of TRI-TAC equipment.

TDC consists of two components: The integrated communications access packages, and the



## Deployable Communications

lightweight multi-band satellite terminal. ICAP provides secure and non-secure voice, non-secure Internet protocol router network and secret Internet protocol router access, fiber optic local area network connectivity, and high capacity (45Mbps) microwave radios to reduce the need for extensive cable runs. The system is compatible with legacy TRI-TAC and the Army's mobile subscriber equipment – critical in the OEF joint and coalition environment. The LMST is a tri-band spoke satellite terminal that operates in the military X-band over the defense satellite communications system, as well as the commercial C- and Ku-bands. Like ICAP, LMST has been fielded to AEF lead wings to permit rapid reachback to the defense information systems network and global information grid. The LMST permits offloading non-critical mission support traffic to commercial satellite systems, freeing the scarce military space segment for more sensitive communications, and providing much needed additional bandwidth.

We were ready after Sept. 11 largely because TDC provided all the tools demanded by the modern warrior in one light and lean package. TDC has proven to be a critical component of the OEF communications architecture, and is performing with unprecedented success. It provides the fast, reliable communications, both as a warfighting tool and a safeguard for deployed airmen who find themselves in harm's way. In the first real test of the Air Force's new communications system, TDC's performance has been superb. OEF is putting a demand on deployed communicators and equipment like we have never seen – and our AEF communicators and communications system are meeting the challenge.

# New technology, 'smart' cards a secure combination for e-mail

By Master Sgt. Daryl Mayer  
*Electronic Systems Center Public Affairs  
Hanscom AFB, Mass.*

In what could be termed a "smarter" way to send e-mail, the Air Force is leaping into the digital age with the advent of the Defense Department public key infrastructure.

PKI uses technology that enables numerous applications such as medium grade service, commonly known as MGS secure e-mail. This application allows everyday unclassified e-mail traffic to be digitally signed and encrypted.

The current e-mail system has some serious flaws, said Chuck Courtney from the Air Force PKI Awareness and Training Office.

"When you receive an e-mail, you really don't know if it actually comes from the person who sent it," he said. "You also can't be sure that someone didn't alter the content of the original message and then forward it."

These are serious problems, especially when dealing with official correspondence, he said.

For instance, if a commander issues a new policy letter, people can see from the signature on the paper, and thus believe with a degree of certainty, that the information is genuine.

And that is the knock against current e-mail systems and one of the stumbling blocks for the move to a paperless Air Force, Courtney said.

While it might seem that e-mail is the ideal medium to replace paper correspondence, the needed security has not been possible, until now. With MGS secure e-mail, this same commander can type the new policy in an e-mail, digitally sign it and send it to every person in the unit, Courtney said.

The process that enables this might seem complicated but it is actually quite simple, he said.

The new identification card being issued throughout the Air Force, commonly referred to as a common access card, uses integrated circuit chips and other means to store information on the card itself.

Once a new message is composed, the user inserts their card into a special card reader installed on their computer, enters their personal identification number and clicks the appropriate icon for digital signature or encryption, Courtney said.

Once encrypted, only the intended recipient can decipher and read the e-mail, effectively allowing two people to securely communicate.

"This is an efficient way to securely process official information," Courtney said.

However secure, MGS secure e-mail is not a substitute for the Defense Messaging System, Courtney said.

But signing e-mails is only the tip of the iceberg, Courtney said. In the near future, authorized users can digitally sign Department of Defense documents and forms.

"This eliminates the need to visit several offices for signed coordination or processing forms," Courtney said. "PKI will be a tool for you to use for electronic signatures on performance reports, travel vouchers and various other applications. It has already been incorporated into the automated business services system."

Another PKI security feature is data integrity, since the system issues a warning when an e-mail message has been modified.

"That way if someone tries to modify your message and forward it on as your original words, the recipient will be signaled that the message has been altered from its original format," he said. "All of these tasks are accomplished by simply clicking on the appropriate icons in the e-mail program toolbar making it easy even for first-time users."

Meanwhile, behind the scenes, the system reads the certificates issued to the user and provides the specific services those certificates grant. There are three certificates that will be issued, Courtney said. The identity certificate is used to digitally sign DOD documents and authenticate secure Web access. The e-mail signature certificate is used to digitally sign e-mail messages and



**The common access card.**

See **SMART CARD** Page 34

# Invisible warriors engage in America's war on terrorism

By Robert Ingram

*Spectrum Manager*

*HQ Air Combat Command*

*Langley AFB, Va.*

Ever since our country declared war on terrorism, Americans have kept up with the latest news as never before. We read about our special forces securing an airfield, see fighters being launched from aircraft carriers, and witness bombs being dropped with pinpoint accuracy. We watch our cargo planes airdrop food to innocent victims, marvel at aircraft refueling in the sky, and see our unmanned aerial vehicles on patrol gathering target data. However, you may not be aware of some invisible warriors performing a vital role in America's war on terrorism.

You won't see these warriors on the front lines, and they won't be mentioned in local headlines or news programs. Yet since Sept. 11, they've played a huge part in America's response to ensure homeland defense. They're Air Combat Command's spectrum managers, controlling a vital resource in America's defense: the electromagnetic spectrum.

In the wake of 9/11, thanks to spectrum managers, our combat air patrols had immediate access to frequencies for command and control, helping to keep America safe from further attacks. Spectrum managers worked with the Air National Guard and 1st Air Force to deconflict frequencies for all CAP missions.

When our military forces

began deploying in support of Operation Enduring Freedom, our spectrum managers were asked to activate the CENTAF/A6-rear spectrum management cell. Deploying Air Force units sent all frequency requests to ACC/SCCF. These invisible warriors at Langley began 24/7 operations and maintained a frequency database of nearly 40,000 frequencies used in the region. This group, consisting of enlisted and DOD civilian personnel, and one contractor, found frequencies for all Air Force units and deconflicted them with frequencies already in use.

These activities might at first sound routine or even boring, until you consider the significance of operations that rely on the radio frequency spectrum for their success. Did you know that special forces can't make an airdrop without frequencies? Or that precision-guided munitions use frequencies to home in on their target? Or that the Predator and Global Hawk UAVs couldn't fly or report their intelligence information without use of the spectrum? In fact, today's military is so high-tech that we can't launch a plane, drop a bomb, gather intelligence or command our forces without uninterrupted use of the radio frequency spectrum. So the next time you read, watch or hear the news about our troops at work in Afghanistan, remember the invisible warriors in the invisible war – spectrum managers on the electromagnetic battlefield.

## SMART CARD

*From Page 33*

the e-mail encryption certificate allows users to encrypt and decrypt messages.

Certificates are valid for three years unless other circumstances are present, such as reassignment, name change, lost CAC, etc.

"It authenticates that a person or system is exactly who or what they claim to be," Courtney said. "It provides data integrity to guard against unauthorized changes to information whether intentional or accidental.

"It prevents a person from later denying that a communication or transaction took place as recorded," he said. "And if you use the encryption, it prevents disclosing information to unauthorized users."

The end result is an infrastructure that is eco-friendly, easy to use, and more secure, Courtney said.

PKI will help alleviate current concerns about traditional mail safety and the burden security measures are placing on the inter- and intra-base mail systems, he said.

Less reliance on paper products means information flows safely and more quickly, even to remote or deployed locations.

The program is being installed on an installation-by-installation basis, Courtney said.

Traveling teams from the Air Force PKI Systems Program Office in San Antonio arrive at a base and within a few weeks common access cards are issued. Card readers and software are then installed on computers and each user and systems administrator is fully trained on using the system.

For more information, go to <https://afpki.lackland.af.mil>.  
(Courtesy AFMC News Service)

# Counsel's O r n e r



**By Joe Hinds**

*Legal Office*

*Air Force*

*Communications Agency*

*Scott AFB, Ill.*

Sergeant Larry Lucky was on temporary duty at a trade show open to the public. An entry fee of \$15, paid for by the Air Force, automatically included entry into a drawing for an all-expense-paid trip to England. After walking through the exhibit hall for an hour, low and behold, Sergeant Lucky's name was drawn as the winner. He was so excited, he raced to a telephone and made flight reservations to London.

Is this a prize Sergeant Lucky may accept? Generally, federal employees must examine these gift horses in the mouth before accepting them. The answer depends on the facts of each case, making it difficult to generalize. Usually, the employee may accept when the contest is open to the public and the employee's entry is not as a result of official duties.

What about this case? Unfortunately, Sergeant Lucky will have to cancel his reservations because the prize was directly linked to his official duties. In other words, his entry fee was paid for by the Air Force and the contest was part of that entry fee.

Would Sergeant Lucky be barred just because

## Ever look a gift horse in the mouth?

he received the prize during duty hours or was wearing a uniform? No, but there might be an appearance problem if he accepts the prize while on duty or in uniform. So under what conditions may he accept a prize? As a general rule, if he wins as a result of stopping at a booth and entering a drawing voluntarily – and accepts the gift while in civilian attire – then he's probably on safe ground.

But don't forget the \$20 limit on gifts from prohibited sources. For example, if Sergeant Lucky had received a \$20 computer training disk at X booth, a \$10 calendar at Y booth, and a \$10 Burger Biggie lunch at Z booth, could he accept the gifts from prohibited sources totaling \$40? Yes, he could accept them because each of the gifts was from a different prohibited source and was valued at or under \$20.

How do you know if the companies are prohibited sources or not? Well, generally a prohibited source is any person or entity doing business or seeking to do business with the Department of Defense. Many, if not all, of the companies at a trade show will fit into this category, so please be careful.

Some of these issues don't have an obvious clear line for you to avoid crossing. When in doubt, please consult your base Staff Judge Advocate for advice.

## Reverse auctions stretch contracting dollars

**By Joe Hinds**

*Legal Office*

*Air Force*

*Communications Agency*

*Scott AFB, Ill.*

Reverse auctions may prove to be the government contract technique of choice in the 21st century. Essentially online suppliers compete for government contracts, using the Internet to "bid" for government business. This process reverses the typical auction process, where the high-

est bidder obtains the product – with the reverse auction, bidders continue to offer lower prices until the lowest bidder prevails.

Unlike the traditional sealed bidding process, where bidders don't know their competitors' bids, in the reverse auction, bidders not only know what their competitors are bidding but actually may underbid them based on that information.

Because technical information is not needed, commercial information technology products

are good candidates for reverse auctions. Even when the contracting officer requires technical information, this may in some cases be obtained from product information off the Internet.

This new process promises speed and another way to stretch your information technology dollars.

For more information and assistance, contact your base contracting office.

