



Med-Alert

The 5th Brigade (HS) Newsletter

July 2001
Volume 17



THE COLONEL'S CORNER

BRIGADE CHRISTMAS CARDS

5th Brigade seeks children's artwork for the Brigade's Christmas Card. We need entries from any child of a soldier of the 5th Brigade. Selected entries will be used to create the Brigade's Christmas cards. Proceeds from the sale of the Christmas cards will support the Family Support Group. Entries should be received by the end of the August Drill (August 19) for selection in September. Preferred artwork should include soldier medics, the 95th Division patch, and reflect the spirit of the holidays. Showcase your child's talents! For additional information contact MAJ Birdwell. Phone number and email address is listed on the unit alert roster.

FROM THE BRIGADE EXECUTIVE OFFICER

Per Colonel Padilla, all staff officers, battalion commanders, and battalion staff officers are to complete the Army's on-line Action Officer Development Course by December 2001.

The Web Address is for the on-line course is:
<http://www.atsc.army.mil/accp/dlsd.htm>



If you click on the ST700 subcourse, you can enroll on-line and get a paper copy or download and work on the computer at your on pace off-line.

This course consists of one subcourse, Action Officer (ST7000), ten lessons with

practice exercises, six appendices, and a final examination.

The course includes lessons and self-graded exercises on: Organizations and Manager's Staff Work; Managing Time and Priorities; Meetings and Interviews; Solving Problems/Making Decisions; Communicating; Writing; Coordinating; Briefings; and Ethics.

The course also contains six appendices to supplement lesson content including: Informal Staff Language; Simpler Words and Phrases; Writing Formats; Time-Saving Tips; Creating Ideas; and Leadership Effectiveness Framework.

For the final examination, you must have a valid Reimer Digital Library (RDL) USER-ID and PASSWORD to access the examination. If you do not, go to the RDL Registration Page on the web at <https://hosta.atsc.eustis.army.mil/register.html> and provide the requested information, and "Register." You will receive email notification of your USER-ID and a "temporary" PASSWORD. You will then need to re-access the RDL Registration Page and change the "temporary" PASSWORD to one of your own creation. Guidance is provided on how to construct your PASSWORD.

NOTE: You must have received ACCD subcourse enrollment verification by e-mail before taking the examination. Read the examination administrative instructions very carefully prior to beginning the examination. Some examinations are timed. Once you complete the examination and "submit" your responses, you will receive immediate feedback of your score. If you obtained a passing score, you will also receive subcourse text references for missed questions.

Your final official grade (Completion Notice) will be provided by e-mail, if available, or first class mail. If you did not obtain a passing score, you may retake the examination after a time lapse of 24-hours from computer processing of your initial attempt.

For questions on course administration (enrollment, final exam, completion certificate, etc.) you may contact TeamB, Army Training Support Center, ATIC-DLS at DSN: 927-5715/2079 COM: 757-878-5715 / 2079 or by e-mail: teamb@atsc.army.mil.

Any other questions can be directed to LTC Lee at 5th Brigade (HS).



TIDBITS

Ladies and Gentlemen:

June our busiest month of the year is over, July is probably the second busiest month as the 10th Bn conducts 3 courses during AT. After July we can focus on other challenges and on improvements to missions conducted. The units are doing a tremendous job and the staff is providing great support to the units.

COL Padilla will be attending his final phase of the War College this month and will be a War College graduate upon concluding this phase. **Congratulations, Sir!!** LTC Lee is the acting Commander in COL Padilla's absence.

ACCREDITATION - The 3457th Medical Training Center was evaluated for accreditation during their AT in the month of June. They performed flawlessly as each of their courses were accredited receiving only 1 comment in 1 course. Way to go 3457th MTC a job well done! The accreditation of the 10th Bn and PND are still on going and thus far they are also doing quite well. In September the final look by the accreditation team will take place and we should hear a final report sometime in October.

ANNUAL TRAINING - As of July 14 the 3457th MTC concluded all their unit missions conducted during annual training. The 10th Bn is currently conducting AT for their 91B30 PH 2 and ANCOC/BNOC. The PND also finished all their AT cycles. Each and every unit has done an excellent job in preparing and executing annual training.

FUNDING - On June 30 the Division consolidated all funds at their level. This is done every year at this time in preparation for yearend close out. What this means to us is that we lost the ability to approve orders at our level. And it means that each and every Request for Order that we send to division will be very closely scrutinized. One thing that division has asked us repeatedly and I ask each and everyone of you is to insure that every soldier has performed or requested to perform their statutory annual training.

FREE MONEY FOR COLLEGE - Military.com's education services has a listing of \$300 million in scholarship funds. All personnel in the military community, including dependents, are encouraged to search the scholarship database. In addition to the scholarship search available, the educational services also provide comprehensive and updated information on educational benefits, such as the G.I. Bill, Veterans Educational Assistance Program (VEAP), and

Survivors' and Dependents' Educational Assistance Program. To access these education services, visit: <http://www.military.com/Careers/Education/0,11754,112,00.html>

OER REPORTS

It is important that all OER reports contain comments regarding promotion, military or civilian schooling, command or level responsibility as stated in the regulation. It is a requirement for the Rater and Senior Rater. Per Andrea Foster, Chief, Evaluations Support Branch, I have worked several reports for the AFS Extension Board and notice this information missing. When we are close to the wire, we have no choice but to reject the OERs with omissions to allow other reports to profile. The soldier as well as the rating chain and the administrative support need to place emphasis on these areas.

ARMY POSTS TO TIGHTEN SECURITY AT ENTRANCES

SSG Marcia Triggs
WASHINGTON (Army News Service, June 11, 2001)

Army installations that have not been stopping vehicles at their front gates will begin limiting public access this summer. "It's important everyone knows that we're not looking to keep people off our installations or to close ourselves in. We want to make sure that people who have intent to do us harm don't enter our installations," said Lt. Col. Bruce Vargo, chief of the Operations Branch for the Army's Security Force Protection and Law Enforcement Division.



An Armywide study revealed that security needed to be tightened on installations, said Lt. Col. Donna Rivera, chief of the Army Physical Security Branch in the office of the Deputy Chief of Staff for Operations and Plans.

Military identification card holders and government employees have until July 31 to register their vehicles with their Provost Marshal Office, Rivera said. Registered vehicles will not be stopped at post gates unless there is a security threat, she said, but others will. Vehicle information will be maintained on an interlinked worldwide Army system, Rivera said. "Once individuals register their vehicles, they will only have to update their unit



designation and address when they move," Rivera said. Drivers of unregistered vehicles will most likely have to present a drivers license, vehicle registration and insurance to gate guards, Rivera said, but added will be up to each installation to mandate what documents will have to be presented. Military policemen will maintain a visitor's log and issue a temporary sign to be placed in the windshield of visitors. Currently there is not a deadline for implementation.

The Physical Security Branch is reviewing ways to help installations get personnel and equipment to meet the requirement, Rivera said. "Some posts will have to build guard shacks and visitor centers. Others may have to close gates or get extra manpower," said Rivera. "It has not been finalized, but we expect to present a course of action by the end of the summer."

Many installations, like Fort Irwin, Calif., are still trying to decide on a plan to implement the policy. "Fort Irwin only has one paved road and the changes to keep it manned won't affect us as much as some larger installations," said Maj. Rob Ali, the public affairs officer at Fort Irwin. "However, we are still working on a detailed mission analysis on how we're going to keep our gates staffed," Ali said. Deciding who is going to stand guard is only part of the plan for Fort Stewart, Ga., which currently has no gates. "Fort Stewart is a totally open post, and we have been trying to get funds to build gates for the last three years," said Don LaRocque, Fort Stewart deputy garrison commander.

"For now, military policemen are placed tactically at main access points." Fort Stewart has been positioning MPs in their humvees at main entrances, LaRocque said, to check identification and vehicle registration. U.S. Army Hawaii has already started to increase security measures, according to 25th Infantry Division (Light) officials. Drivers in Hawaii were required to register their vehicles by May 11, and long-term plans at Schofield Barracks include the construction of additional access control measures including closed circuit television and other monitoring devices, according to officials.

The controlled access policy is a Department of Defense directive that the Army is re-enforcing after a study revealed that a significant number of Army installations were not monitoring their entrances, Rivera said. "Last Spring the vice chief of staff [Gen. John Keane] wanted to know how many installations have controlled access and the limitations of the access," Rivera said. "We conducted a study and found out that most overseas posts have controlled access. However, U.S. Army installations have a more

relaxed posture than any of the other services." Based upon the findings Army security is being increased. "We don't know where people may attack, and the bombings in Oklahoma City and at the World Trade Center [New York City], give credence that we can be hit on the home front," Rivera said. "Monitoring people who enter and exit installations is the best deterrent against attacks," Vargo said. "It protects us from terrorists, criminals and during civil disturbances and natural disasters. Registered vehicles are the first step in this line of defense, and it will also help expedite the flow of traffic at gates, Vargo said. However, on days when traffic seems to be congested at the gates, the community should feel safer, he said. To help with the flow of traffic, Rivera said, people should coordinate with internal security if they are expecting guests for official functions and ceremonies. Other tips are not to schedule arrival times during peak hours of congestion and to tell visitors to have proper identification and documents handy.

3457TH CIP REMINDER

The Bde staff, under the leadership of LTC Lee, will be conducting the Command Inspection Program (CIP) for the 3457th on 8 September 01.

90-DAY EVENT CALENDAR

19 July	Start 91 CMF BNCOC/ANCOC
16 - 20 July	NTCC, 91W PAT Briefing
21 - 22 July	Bde HQs Drill
3 - 4 August	USARC Readiness Briefing
6 - 9 August	Division Personnel SAV
11 - 12 August	10th Bn CIP
11 - 12 August	3457th MTC & 10th Bn Drill
18 - 19 August	PND & Bde Drill
22 - 23 August	10th BN ISE Meeting
8 - 9 September	3457th MTC and 10th Bn Drill
8 - 10 September	10th Bn MOBEX
8 September	3457th CIP (this is a change)
15 - 16 September	HQs and PND Drill
15 September	PND CIP

AUTOMATION MONITORING

By Steve Hara
WASHINGTON (American Forces Press Service, June 25, 2001)

Defense Department computer security systems



and specialists foiled nearly 22,500 would-be intruders in 1999 and 24,500 in 2000. There's no let-up in sight. Special agent Jim Christy said he and others on his law enforcement staff are in a "growth business" chasing hackers and spies and running other criminal activities to ground. As representatives of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, they also counsel DoD employees on being an effective first line of defense instead of the weakest link. When he discusses computer security, Christy said, he drives home that average folks aren't expected to mount an ironclad defense. Rather, he stressed, they can do simple things that make life harder for bad guys -- and stop doing simple things that make life easy for them.

Use different passwords at Web sites and on every machine you use.

Reject all site and system offers to "remember" you and your password. Bad guys know many people use just one password, so attacking an easily hacked site gives them "skeleton keys" to tough ones.

Don't open e-mail attachments from people you don't know, and don't open them uncritically just because someone you do know supposedly sent them. Hackers use attachments to inject viruses and other mischievous or malicious computer code into machines and systems. A common means to spread infections is by sending e-mail copies to everyone in a victim's address book -- using the victim's name.

Log off or lock your workstation when you go on breaks or out to lunch. No point giving bad guys unfettered access to your computer and network -- and leaving you holding the bag because the system thinks you're at the keyboard.

Never use personal diskettes, Zip disks and the like on classified systems. Computers divide files and write them to disk in units called sectors. If the file's last sector is only partially filled, the machine tops it off with data randomly pulled from memory or hard drives -- there's no real telling in advance where the information might come from. So writing and saving even your holiday greetings letter on a classified system is a potential disaster. That's why the practice is a security violation.

You can be a security risk even if you don't work with classified files, have none on your computer and have no access to any. The mindset on the last point is wrong for at least three reasons, Christy noted. First, too many people think a secure system can't be

hacked from their office computer network -- usually because they themselves don't know how. Fact is, good hackers really can launch attacks on your lowly machine if you give them the time and opportunity, he said. Second, he continued, intelligence analysts make a living by drawing conclusions and educated guesses from bits and pieces of unclassified and seemingly unrelated information. Third, information doesn't have to be classified to be sensitive. Medical records, personnel records and personal address and phone books aren't usually classified, but all contain data protected from public release by the Privacy Act of 1974. Good security, he said, means locking out all snoops, not just spies. Christy and company's growing business in security issues gives constant rise to another: personal privacy. You have none, and that roils many employees. Uncle Sam's machine, Uncle Sam's rules, Christy noted. Agency systems administrators are supposed to have the means to track every move made by every user in their realm. Literally. Every keystroke. Every mouse click. They can reconstruct any document you write, every Web site you visit, Christy said.

Monitoring could be used to detect crimes and employee waste and abuse, but rarely is, he noted. More frequently, investigators and managers consult monitoring records to make or break cases after allegations surface other ways. Computer users can't claim a "probable cause" defense after being caught, because they all agree to be monitored as a condition of access. "There is absolutely no privacy on a government computer," Christy said. "Every time you turn one on, you get a message that the government can and will monitor you, and if you sign in, that means you understand and agree. Always assume you're being monitored."

YOUR CHAIN OF COMMAND

5th Brigade (HS)	
COL Angel Padilla	CSM Alfred Habelman
10th BN	
MAJ James Hickey	CSM Paul Castro
3457th	
LTC Floyd Priester	CSM Vacant
PND	
MAJ Mary Gomez	CSM David Stading
HHD - 5th Brigade	
CPT Mario Avila	SFC Dan Carlin