



REPLY TO  
ATTENTION OF

**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, 21ST THEATER SUPPORT COMMAND  
UNIT 23203  
APO AE 09263

AERIM

15 September 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 21st Theater Support Command Policy Letter 20, Information Assurance

1. Reference Headquarters, United States Army Europe and Seventh Army, USAREUR Command Policy Letter 4, Information Assurance, 4 May 2003.

2. Information assurance is the cornerstone to the integrity and cohesiveness of our warfighting capabilities. The Commanding General, Headquarters, United States Army Europe and Seventh Army directed subordinate Commanders to enhance the theater-wide information assurance posture.

3. Information assurance training is essential to meet head-on all threats against our automated systems.

a. The Command Information Assurance Manager has developed and disseminated an Information Assurance/Security Awareness Training and User Password Protection briefing presentation to each of the headquarters staff sections and brigade information assurance managers. Information assurance is a commander's program. Commanders and staff principals will provide this Information Assurance/Security Awareness Training to your subordinates down to the lowest echelon possible. Training will be conducted on a bi-annual basis and indicated on your respective training schedules.

b. I also direct that information assurance managers and officers, at all echelons, train your staff to set and activate password protected screen savers and enforce the locking of the workstations when left unattended. Protecting data from those whom do not have a need to know is critical. Inform your users that just because they have a password protected screen saver activated, they must still lock their workstations when they walk away from them.

4. Secure computer configuration and installation of authorized software is another way to protect our automated systems. Only systems meeting the Regional Computer Emergency Response Team, Europe hardware and software security baseline configuration will be authorized on the 21st Theater Support Command (TSC) network. Only authorized software will be installed on Government owned computers. Government owned central processing units, monitors, laptop computers, printers, and other peripherals and Government leased equipment, such as copiers, will have the appropriate labels applied to them in clearly visible locations that

AERIM

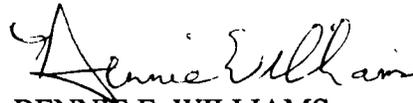
SUBJECT: 21st Theater Support Command Policy Letter 20, Information Assurance

will not hamper their operation. These labels serve as reminders to equipment users as to the classification level of that particular piece of equipment. The labels will be applied to the equipment in all environments, single and mixed classification processing areas.

5. The Internet and Intranet are valuable tools developed to make our jobs easier. In light of the recent force protection measures, webmasters and web developers will ensure that personal information is not contained on any of the 21st TSC web pages. Generic e-mail addresses will be used rather than the personal e-mail addresses. Questions regarding new web page procedures may be addressed to the 21st TSC Webmaster at [webmaster@hq.21tsc.army.mil](mailto:webmaster@hq.21tsc.army.mil).

6. The Command Information Assurance Manager (CIAM) is here to support you. If you have questions or require assistance, please contact the CIAM at [ia@hq.21tsc.army.mil](mailto:ia@hq.21tsc.army.mil).

7. FIRST IN SUPPORT!



BENNIE E. WILLIAMS  
Major General, USA  
Commanding

DISTRIBUTION

A (21st TSC Cir 25-30)