



**DEPARTMENT OF THE ARMY**  
**HEADQUARTERS, UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY**  
**THE COMMANDING GENERAL**  
**UNIT 29351**  
**APO AE 09014-9351**

AEAIM-IAPM

4 May 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army in Europe Command Policy Letter 4, Information Assurance

1. Reference AR 380-19, Information Systems Security, 27 February 1998.
2. Our warfighting capability greatly depends on the integrity of our automated information systems. These systems give us the leading edge in information dominance by enabling us to make effective operational decisions. These systems, however, are being attacked every day. External threats range from casual weekend hackers to state-sponsored attacks by those trying to alter or exploit our data. Our best defense against these attacks is information assurance.
3. Information assurance protects our automated information systems and preserves the integrity of our information. For information assurance to be effective, every member of the command and staff must understand the security risks involved in using a computer and the responsibility involved in running a network with secure functions. In addition, everyone who uses a computer must know how to recognize and respond to attacks on our systems. This requires training and certification. Commanders have the lead in raising unit awareness of this requirement.
4. Information assurance includes measures we take to protect our data and information systems. The following key fundamentals of information assurance will maximize this protection:
  - a. **A Trained Workforce.** Commanders will ensure that all information technology professionals complete the USAREUR Information Assurance/Computer Network Defense Training Program.
  - b. **Secure Computer Configurations.** USAREUR computer security baselines (available on the USAREUR Information Assurance (iAssure) website at <https://iassure.usareur.army.mil>) will be applied to all computer systems on all USAREUR networks. Configuration changes directed by information assurance vulnerability alerts (IAVAs) issued by the USAREUR G3 must be accomplished by the dates specified in the IAVAs. Organizations that fail to comply with IAVA requirements may be disconnected from all networks until corrective actions have been taken.
  - c. **Self-Checks for Compliance.** Each unit will scan its local area network (LAN) at least once every 6 months for known vulnerabilities. Units will also scan their LANs within 10 days after an IAVA has been issued to ensure that all affected systems are identified for action. System administrators will maintain and review system-security logs to identify suspicious activity.

*This letter is available at <https://www.aeaim.hqusareur.army.mil/library/home.htm>.*

AEAIM-IAPM

SUBJECT: Army in Europe Command Policy Letter 4, Information Assurance

5. Most computer intrusions into our networks can be prevented if all users comply with the fundamentals described above. Commanders will monitor compliance with these fundamentals through command inspection programs and management controls. Commanders may also monitor compliance through semiannual and quarterly training briefings. The iAssure website at <https://iassure.usareur.army.mil> provides a suggested slide for briefing the fundamentals of information assurance.

6. In addition to the iAssure website, the USAREUR Information Assurance Program Manager, 5th Signal Command, the Regional Computer Emergency Response Team - Europe, and unit information assurance managers all provide tools, training, and assistance to help organizations and individuals enforce the fundamentals of information assurance.

7. Leaders must enforce information assurance. Every individual in USAREUR who uses a computer is a target for our adversaries. I therefore expect every individual to be trained, ready, and proficient in assuring the security of our information systems.



B. B. BELL  
General, USA  
Commanding

DISTRIBUTION:  
A (AEPUBS)