



DEPARTMENT OF THE ARMY  
HEADQUARTERS, U.S. ARMY ARMOR CENTER AND FORT KNOX  
FORT KNOX, KENTUCKY 40121-5000

REPLY TO  
ATTENTION OF:

ATZK-IM (380)

20 September 2001

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters  
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Thunderbolt Six Policy Memo No. 38-15 – Information Assurance (IA) Program

1. References:

- a. Public Law 100-235, the Computer Security Act of 1987.
- b. AR 380-19, Information Systems Security, 27 February 1998. This regulation is due to be replaced with AR 25-IA, Information Assurance.
- c. Message, HQDA, SAIS-IAS, 160639Z Dec 98, subject: U.S. Army Systems Administrator Certification Training.
- d. DODI 5200.40, Department of Defense Information Technology Certification and Accreditation Process (DITSCAP), 30 December 1997.

2. The purpose of this memorandum is to express command policy of compliance with all laws and regulations governing the Information Systems Security/Information Assurance (ISS/IA) Program. This program requires our full attention to ensure that our computer network is protected and that the information on our network is not changed or contaminated.

3. The Computer Security Act of 1987 requires the establishment of a computer security program for all "Federal computer systems." The term "Federal" applies to all computer systems operated by a Federal agency or by a contractor of a Federal agency or any organization/activity that processes information on behalf of the Federal Government.

4. Addressees will appoint an individual in their organization to serve as the Information Assurance Security Officer (IASO) and be responsible for implementing ISS/IA requirements and responding to the installation's Information Assurance Manager. Before any system is placed in use or individuals allowed access, the following actions must be completed:

- a. The system must be accredited in accordance with applicable regulation.
- b. The equipment must be engraved to protect from theft.

ATZK-IM

SUBJECT: Thunderbolt Six Policy Memo No. 38-15 – Information Assurance (IA) Program

- c. Current anti-virus software must be loaded and continuously updated and running.
  - d. DOD warning banner must be installed.
  - e. Risk Assessment must be prepared as part of System Security Accreditation.
  - f. Each user must have appropriate level of investigation, be issued ID and Password, and receive an initial briefing concerning their security responsibilities.
5. Individuals assigned the duties and responsibilities as IASO, systems administrator (SA), or network manager (NM) will be trained and certified.
- a. IASO certification will consist of completion of the Information Assurance Security Officer Computer Based Training Course and the three DISA training CD ROMs (INFOSEC Awareness, OISS Volume 1 and OISS Volume II), or the Information Assurance Security Officer Certification Course.
  - b. SAs/NMs will be trained and certified in accordance with reference c above.
6. The following is provided as generic guidance for conducting Risk Assessments on Information Systems (IS). Actual Risk Assessments will vary from system to system.
- a. Risk assessment is the process of analyzing the threats, vulnerabilities, security requirements, and available safeguards for an information system with regard to the potential impact that the loss of that information or system's capabilities would have on national security. It must evaluate the likelihood of unauthorized disclosure of information, denial or degradation of service, unauthorized manipulation of information, or unauthorized use. A Risk Assessment is required in the DITSCAP validation phase (Phase 3) as Appendix G of the System Security Authorization Agreement. Risk Assessments are also part of the risk management program required by AR 380-19.
  - b. The Risk Assessment must address the adequacy of the physical, administrative, procedural, and automated security mechanisms that are relied on to ensure secure system operation. To assess the effectiveness of the overall security of the system, the Risk Assessment must examine the system's generic system threats, the results of the certification testing, and the risk mitigation measures that have been developed. The Risk Assessment report will include the following:
    - (1) System Vulnerabilities. Vulnerabilities are weaknesses in system design, security procedures, implementation, and internal controls that could be exploited. As a minimum, all security-related shortcomings discovered in the system certification process must be addressed in the Risk Assessment.

ATZK-IM

SUBJECT: Thunderbolt Six Policy Memo No. 38-15 – Information Assurance (IA) Program

(2) Threats. The Risk Assessment must identify the threats that can be applied to each system vulnerability. A threat is an event or method that can potentially compromise the integrity, availability, or confidentiality of an information system. These threats include both authorized and unauthorized users and include both deliberate and accidental acts.

(3) Threat-Vulnerability Match. The Risk Assessment must match one or more threats to each vulnerability. In the event that a threat cannot be identified for a vulnerability, that vulnerability may not pose risk to the system.

(4) Security Requirement. The security requirement associated with each vulnerability must be identified.

(5) Safeguard. A countermeasure must be identified to mitigate the risk associated with each threat-vulnerability match.

(6) Risk Statement. A statement of the risk associated with each threat-vulnerability match and its countermeasure shall be provided.

(7) Finally, a statement must be made summarizing the overall security posture of the system. This statement will be provided to the system's Designated Approving Authority (DAA) with one of the following accreditation recommendations:

(a) Accredite the IS or local area network (LAN) for processing in a particular mode of operation for a certain classification level. This certifies that the security posture of the IS or LAN is very high and the residual risk is at an acceptable level.

(b) Grant an interim approval to operate (IATO) for a period of up to 1 year while additional security safeguards are installed. This certifies that the security posture of the IS or LAN requires enhancement due to a high level of residual risk.

(c) Deny approval to operate, if the IS or LAN has a very low security posture and the residual risk is unacceptable.

7. The Director of Information Management is the Information Assurance Manager (IAM) for Fort Knox and is responsible for the ISS/IA program. His staff will conduct audits/reviews of systems to ensure provisions of paragraph 3 above are being implemented and comply with law and regulations. These reviews will be coordinated with organization IASOs.

ATZK-IM

SUBJECT: Thunderbolt Six Policy Memo No. 38-15 – Information Assurance (IA) Program

8. Your support for the ISS/IA program is essential to protecting the Fort Knox computer network from illegal and damaging activity. Without appropriate security procedures, our network and information will become contaminated and useless. To ensure continued confidentiality, integrity, and availability of our information we must protect our information technology assets.



R. STEVEN WHITCOMB

Major General, USA

Commanding

DISTRIBUTION:

C plus

25 – ATZK-IM

CF:

DCG, USAARMC

CDRs, Fort Knox Partners in Excellence