

DEPARTMENT OF THE ARMY  
 HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND  
 5001 EISENHOWER AVE, ALEXANDRIA, VA 22333-0001

AMC MEMORANDUM  
 No. 380-23

30 October 2003

Information Assurance  
 U.S. Army Materiel Command (AMC)  
 Information Assurance (IA) Training Policy

|                       | Paragraph | Page |
|-----------------------|-----------|------|
| Purpose.....          | 1         | 1    |
| Scope.....            | 2         | 1    |
| Responsibilities..... | 3         | 1    |
| Policy.....           | 4         | 1    |
| Point of Contact..... | 5         | 3    |
| References.....       | 6         | 3    |

**1. Purpose:** This memorandum provides additional policy guidance and information about the AMC IA training program.

**2. Scope:** This memorandum is effective immediately and applies to all AMC activities within Headquarters AMC, its Major Subordinate Commands (MSCs), and Separate Reporting Activities. This memorandum rescinds AMC Information Assurance (IA) Training Guidance Memorandum, 26 February 2002. All certification requirements are described in the Appendix.

**3. Responsibilities:** The AMC Information Assurance Program Manager (IAPM), MSC Information Assurance Managers (IAMs), Installation IAMs and Information Assurance Security Officers (IASOs) will ensure the execution of this policy and guidance within their respective activities.

**4. Policy:**

a. In addition to the requirements outlined in AR 25-2 and ASD Memo, 15 July 2003, all AMC organizations will ensure IA training is completed by all personnel, to include users/operators, IA personnel, system administrators and network managers. All IA personnel will register and maintain their training information in the Information Assurance Vulnerability Alerts (IAVA) Compliance Reporting Database (CRD) <https://informationassurance.us.army.mil/>. After login, click the "IAO Login" link to request an IAO account or login to the database. After completion of any IA training personnel will update their records within 10 working days.

b. The AMC User Information Assurance training will consist of at least one of the following:

(1) The Defense Information Systems Agency (DISA) CD-ROM “Information Assurance Awareness which is available from the DISA Information Assurance Support Environment (IASE) IA Training Products website at: <http://iase.disa.mil/eta/>.

(2) Completion of the User Security Course located at the Fort Gordon Information Assurance website at: <http://ia.gordon.army.mil/iss/Index.htm>.

(3) Locally developed Information Assurance training. In order for locally developed training to fulfill this requirement it must meet the minimum levels of expected training as outlined in AR 25-2.

(4) Users will receive annual refresher training as a minimum or as conditions warrant.

c. System Administrators (SA)/Information Assurance Network Managers (IANM)/Information Assurance Network Officers (IANO) will complete Level I certification training before they are given “administrator” or “root” level access or made a member of any administrative groups. If Level I training has not been completed and annotated in their training information in the Compliance Reporting Database (CRD), the SA/IANM/IANO “root” or “administrator” level access will be suspended until the training is completed.

d. The 10-day SA/IANM course required for Level II certification is the Fort Gordon School of Information Technology “System Administrator/Network Manager Security Course”, Army Training Requirements and Resources System (ATRRS) Course Number: 7E-F66/531-F21. Information on this course can be found at the Fort Gordon School of Information Technology website: <http://ia.gordon.army.mil/sysadmin.htm>. Information on the ATRRS can be found at <http://www.atrrs.army.mil/>. It is possible to waive the 10-day SA/IANM Level II training requirements. Individuals should submit a waiver request, with transcripts from their related coursework, to their local IAM. The packaged should then be endorsed locally and forwarded through the local chain of command, the MSC and the AMC IAPM to HQDA. If the waiver is approved, HQDA will grant Level II certification.

**NOTE:** Successful completion of the Level III course managed by the National Guard Bureau or U.S. Army Reserve will fulfill Level II certification requirements.

e. The IAPM, whose position is assigned to HQ AMC and is appointed by the HQ AMC Chief Information Officer (CIO), must complete the IAM course within 6 months of their appointment date. Details on the availability of the IAM Course can be found on the Army’s Information Assurance website: <https://informationassurance.us.army.mil/>. After login, click Information Assurance Training > Information Assurance Manager Course. Information can also be found on the Fort Gordon Information Assurance website: <http://ia.gordon.army.mil/iam.htm>. Other Army-approved methods include Army E-learning/CBT modules. Or other Service or Agency equivalent.

f. All Information Assurance Security Officers (IASO) must complete an IASO course within six months of their date of appointment. This training is available online at the Fort Gordon website: <http://ia.gordon.army.mil/>, or on CD-ROM – DISA’s Operational Information Systems Security (OISS) Volumes 1 & 2, available from the DISA Information Assurance Support Environment (IASE) IA Training Products website at: <http://iase.disa.mil/eta/>. In addition, completion of the Information Assurance Manager course will fulfill this requirement.

g. A newly appointed Designated Approving Authority (DAA) will complete the DISA Designated Approving Authority (DAA) CD-ROM training that is available from the DISA Information Assurance Support Environment (IASE) IA Training Products website at: <http://iase.disa.mil/eta/>.

h. Refresher training for IAPMs, IAMs, IANMs, IASOs, and SAs will be attendance at an Army IA workshop every 18 – 24 months, attendance at DoD-sponsored IA workshops, completion of modules in Army E-learning/CBT IA learning path, or approved commercial courses.

i. The IAPM, IAMs, IASOs, SAs, and IANMs can substitute other Service or Agency courses to fulfill certification requirements. The course must be identified in the CRD and all pertaining information provided.

## **5. Point of Contact (POC):**

The AMC POC for this memorandum is the HQ Information Assurance Program Manager (AMCIO-P), Commercial: (703) 617-3372 or DSN: 767-3372, e-mail: [amcio-iapm@hqamc.army.mil](mailto:amcio-iapm@hqamc.army.mil).

## **6. References:**

- a. Army Regulation 25-2, Information Assurance, 17 September 2003
- b. ASD Memo 15 July 2003, “DoD Information Assurance/Information Technology Designated Approving Authority (DAA) Training and Certification Requirements”

The proponent of this memorandum is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMCIO-P, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

RICHARD A. HACK  
Lieutenant General, USA  
Deputy Commanding General

MICHAEL D. COLTON  
Chief, IT Programs & Support Division

DISTRIBUTION:

B

H

[amciainst@hqamc.army.mil](mailto:amciainst@hqamc.army.mil)

[amc-ia-mscgroup@hqamc.army.mil](mailto:amc-ia-mscgroup@hqamc.army.mil)

**APPENDIX**  
**Information Assurance Training/Certification Level Matrix**

| Position | Number Required                   | Basic Responsibilities  | Training/Certification Required   | Training Source  |
|----------|-----------------------------------|---|---|--|
| IAPM     | One appointed at each ARMY MACOM. | (a) Direct MACOM’s management of the computer security program<br>(b) Develop command-unique guidance as required.<br>(c) Responsible for all Automated Information Systems (AIS) accreditation procedures within the command.<br>(d) Establish and oversees the IA training programs within the command.<br>(e) Approval authority for AIS to operate (on behalf of the MACOM Commander).<br>(f) Administer management evaluation controls and IA inspection programs. | Complete the Army Information Assurance Manager (IAM) Course within 6 months of their appointment.  | In residence course. Other Army-approved methods include Army E-learning/CBT modules. Or other Service or Agency equivalent.   |
| IANM     | Appointed at each ARMY MACOM.     | (a) Provide direct support to the MACOM IAPM in matters of network security.<br>(b) Implementation of the command Information Assurance and Vulnerability Assessment (IAVA) programs.<br>(c) Serve as the alternate IAPM as required.<br>(d) Develop and staff IA technical policy and procedures for MACOM unique systems.   | (1) Complete the IAM Course and<br>(2) Complete the System Administrator/ Network Manager Security Course (Level II) within 6 months of appointment | Introductory training can be: IA Workshop, IASO Course, IAM Course, include Army E-learning/CBT modules, DISA OISS CD, DISA DoD IA Awareness CD. Level II Course is in residence. Personnel in IANM positions are authorized to take substitute courses to fulfill Level II certification requirements |

| Position | Number Required  | Basic Responsibilities   | Training/Certification Required                                | Training Source  |
|----------|--|--|--|--|
| DAA      | <p>HQ AMC CIO appointed as DAA for the MACOM.<br/>Others appointed at levels below MACOM as necessary.</p> | <p>(a) The security of the information systems under their command.<br/>                     (b) Granting formal acceptance of the computer system's security.<br/>                     (c) The issue of accreditation/ reaccreditation statements.<br/>                     (d) Enforce management controls.<br/>                     (e) Ensure cost-effective security of automated information systems (AIS).<br/>                     (f) Ensure adequate supervision of AIS.</p>   | <p>Complete the DAA computer-based training course.</p>        | <p>Current course is version 2 dated May 2002 and is available from the DISA Information Assurance Support Environment (IASE) IA Training Products website at: <a href="http://iase.disa.mil/eta/">http://iase.disa.mil/eta/</a></p> |
| IAM      | <p>Appointed as needed at all appropriate levels of command.</p>   | <p>(a) Establish and implement the IA program for all AIS within their command or activity and for AIS under development.<br/>                     (b) Oversee the IA training and awareness program.<br/>                     (c) Ensure an IASO is appointed for each separate AIS, group of AIS, or network.<br/>                     (d) Establish an Army IA Program for protecting all information systems for which they are accountable.<br/>                     (e) Ensure all AIS and/or networks are accredited.<br/>                     (f) Review threat and vulnerability assessments.<br/>                     (g) Report security incidents and technical vulnerabilities.<br/>                     (h) Establish responsibilities for each assigned IASO.</p> | <p>Complete the IAM Course within 6 months of appointment.</p> | <p>In residence course</p>   |

| Position | Number Required  | Basic Responsibilities  | Training/Certification Required   | Training Source   |
|----------|--|---|---|---|
| IANO     | Appointed as needed by the Garrison Commander or manager of the installation or activity responsible for the network at all appropriate levels of command below MACOM. | (a) Provide direct support to the IAM.<br>(b) Implementation of the IA program for networks to ensure the military information environment (MIE) is operational and secure by developing, issuing and implementing security procedures and protocols governing network operations.  | Complete the IAM Course within 6 months of appointment.                   | In residence course   |
| IASO     | Appointed by the commander or manager/director of the activity responsible for the as needed.  | (a) Day-to-day security implementation and related administrative duties.<br>(b) Ensure systems are operated IAW governing directives.<br>(c) Ensure all personnel are cleared prior to accessing any AIS.<br>(d) Report security incidents, technical vulnerabilities, criminal activity and foreign intelligence to the IAM.<br>(e) Review all system changes to determine the security impact on that particular AIS and other systems it may affect.<br>(f) Prepare or oversees the preparation of certification and accreditation documentation.<br>(g) Maintain a password system, oversees the review of system audit trails and maintains access control records. | Complete an IASO Course or the IAM Course within 6 months of appointment. | The IASO Course can be completed by the web based ( <a href="http://ia.gordon.army.mil/ia-so/default.htm">http://ia.gordon.army.mil/ia-so/default.htm</a> ) or the DISA Operational Information Systems Security (OISS) Volume 2 CD dated May 1998. Other means of certification include completion of the IAM course, Army E-learning/CBT IA modules or MACOM (or other Service) course. |

| Position | Number Required  | Basic Responsibilities  | Training/Certification Required  | Training Source  |
|----------|--|---|--|--|
| SA       | Appointed for each Information System (IS) or group of IS as needed. | (a) Ensuring supported systems are configured properly and the appropriate security features are enabled for the level of the system.<br>(b) Information Assurance Vulnerability Alert (IAVA) compliance for supported systems.<br>(c) Monitoring of supported systems ensuring reliable and secure performance of infrastructure resources.                                    | (1) Complete introductory training (Level I) and<br>(2) Complete technical training (Level II) 10-day SA Security Course within 6 months of assuming position.<br>(3) Complete advanced training (Level III) as required | Introductory training can be: IA Workshop, IASO Course, IAM Course, DISA OISS CD, DISA DoD IA Awareness CD. Level II Course is in residence. Personnel in SA positions are authorized to take substitute courses to fulfill Level II certification requirements.                         |
| User     | N/A  | (a) Become familiar with and follow established security and information assurance policies.<br>(b) Do not use government-owned automated information systems (AIS) for anything other than official government business.<br>(c) Remain diligent concerning the proper use of government AIS.<br>(d) Report suspected/actual security violations to your IASO and/or help desk. | (1) Complete an initial user training program prior to receiving network access<br>(2) Complete annual refresher training  | User training can be: The DISA DoD IA Awareness CD or the online user course at ( <a href="http://ia.gordon.army.mil/is/Index.htm">http://ia.gordon.army.mil/is/Index.htm</a> ). Also, locally developed training can be used as long as minimum requirements listed in AR 25-2 are met. |