

18 August 2005

**Information Management – Management of Subdisciplines  
INFORMATION ASSURANCE (IA)**

---

**Summary.** This supplement provides policy and mandates procedures for implementing the Army IA Program within TRADOC.

**Applicability.** This supplement applies to all TRADOC activities and to installations with a TRADOC Senior Mission Commander.

**Suggested improvements.** The proponent of this supplement is the Chief Information Officer (CIO). Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, TRADOC (ATIM-I), 84 Patch Road, Fort Monroe, Virginia 23651-1051. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

**Supplementation.** Further supplementation is prohibited unless specifically approved by Commander, TRADOC, (ATIM-I), 84 Patch Road, Fort Monroe, Virginia 23651-1051.

**Availability.** This publication is distributed through the TRADOC Homepage at <http://www.tradoc.army.mil/tpubs/supplndx.htm>.

---

AR 25-2, 14 November 2003, is supplemented as follows:

**Paragraph 2-7, Commanders of MACOMs; Chief, Army Reserve (CAR); Chief, National Guard Bureau (NGB); program executive officers (PEOs); direct reporting program managers; NETCOM RCIOs; direct reporting units (DRUs); Installation Management Agency (IMA); and the Administrative Assistant to the Secretary of the Army.**

2-7e (Add the following):

(1) Subject to the restrictions below, TRADOC General Officers and Senior Executive Service personnel may appoint DAAs for ISs their activities have developed and for ISs and networks under their control for which DAAs have not been appointed in chapter 5 of this regulation or by other DoD or DA guidance. Copies of DAA appointment orders shall be forwarded to the TRADOC IAPM ([tradociapm@monroe.army.mil](mailto:tradociapm@monroe.army.mil)).

(a) The Army G-2 is the accreditation authority for Sensitive Compartmented Information (SCI) systems operating at Protection Level 1 or 2, and CIO/G-6 is the accreditation

## TRADOC Suppl 1 to AR 25-2

authority for Special Access Program systems. TRADOC oversight for ISs processing SCI remains with the TRADOC Deputy Chief of Staff for Intelligence.

(b) TRADOC CIO is the DAA for ISs that transmit data outside of installation network boundaries and are hosted on TRADOC-managed servers. Director, Enterprise Systems Technology Activity (ESTA) is the DAA for ISs that transmit data outside of installation network boundaries and are hosted on NETCOM- or DOIM-managed servers.

(c) General Officers and Senior Executive Service personnel may accredit Top Secret collateral systems operating in a dedicated or system high security mode.

(d) Colonels/GS-15s and above occupying command or principal staff position may accredit Secret and Confidential ISs operating in a dedicated or system high security mode.

(e) Lieutenant Colonels/GS-14s and above may accredit sensitive systems operating in a dedicated or system high mode of operation.

(2) Prior to assuming DAA responsibilities, personnel shall minimally complete the DoD DAA computer-based training (CBT) product. The CBT, titled, "DAA, Designated Approving Authority," can be obtained from DISA at <http://iase.disa.mil/eta/index.html>. The course completion certificate, also available at the DISA website, shall be E-mailed to the TRADOC IAPM ([tradociapm@monroe.army.mil](mailto:tradociapm@monroe.army.mil)), who will forward it to CIO/G-6 to meet DA requirements.

(3) DAA responsibilities include the following:

- (a) Grant approval to operate an IS or network in a specific security mode.
- (b) Review documentation and sign accreditation statement for the IS or network.
- (c) Verify that the IS or network complies with security requirements.
- (d) Confirm that residual risks are within acceptable limits.
- (e) Approve classification level required for applications implemented in a network environment.
- (f) Approve additional security services necessary to connect external systems.
- (g) Define the criticality and sensitivity levels for each IS or network.
- (h) Allocate resources to achieve an acceptable level of security and to remedy security deficiencies.
- (i) Establish working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation.

(j) Ensure, when classified or sensitive information is exchanged between logically connected components, the information protected from unauthorized observation.

**Chapter 2, Responsibilities.**

After paragraph 2-16, add:

**2-17. Senior Mission Commanders.** Information Assurance is a Force Protection (FP) issue. Senior Mission Commanders provide executive oversight of their installation IA program. Senior Mission Commanders will ensure that—

- a. TRADOC priorities are conveyed to the installation.
- b. The requirements of this regulation are aggressively enforced.
- c. An appropriate percentage of available resources are applied to network defense. The security of Army information must be ranked high in the competition for available resources.

**2-18. Installation Commanders.** Installation Commanders have overall FP and IA compliance responsibility for the installation. They provide operational oversight of the installation's IA program and set the installation's IA priorities. Installation Commanders will ensure that—

- a. Information Assurance is integrated into their overarching installation FP program.
- b. The requirements of this regulation are aggressively enforced.
- c. The installation is adequately staffed with qualified and trained personnel to execute the IA responsibilities crucial to an effective FP program.
- d. All installation tenants comply with this regulation and other IA policies.
- e. The Installation Operations Center (IOC) has the ability to immediately notify and recall all assigned installation and tenant IA personnel.
- f. The supporting Installation Management Agency Region is informed of Installation Commander IA policies that will affect all tenants.

**Paragraph 3-2, Information Assurance personnel structure.**

Add subparagraph g:

g. *Information Assurance POC.* Commanders, managers, and directors of activities will appoint an IA POC (either an IAM or an IASO, as appropriate) and ensure that the POC's name, phone number, E-mail address, training status, and other required information are entered into the Asset & Vulnerability Tracking Resource (A&VTR) database. IAM and IASO

## **TRADOC Suppl 1 to AR 25-2**

responsibilities can be an additional duty or a full-time position, depending on the level of complexity of the activity's ISs, and are outlined in subparagraphs d and f above, respectively.

### **Paragraph 4-3, Information Assurance training.**

4-3a(8) (Add subparagraph (c)):

(c) Commanders, managers, and directors of activities will ensure that mandatory IA user training is conducted as described in subparagraphs (a) and (b) above.

### **Paragraph 4-21. Information system incident and intrusion reporting.**

Add subparagraph e:

e. Installation Commanders will ensure that—

(1) They are thoroughly informed about all suspected and confirmed IS intrusions on their installations.

(2) All suspected and confirmed intrusions are reported to the IOC.

(3) Within two hours of discovery of a suspected or confirmed intrusion, the IOC submits a Suspected or Confirmed Compromised Computer or Network Intrusion Report to TRADOC Operations Center IAW TRADOC Command Guidance 04-001.

(4) Appropriate installation personnel conduct a thorough FP/OPSEC assessment for all intrusions. This assessment should begin immediately upon determination that an intrusion may have occurred. The purpose of the assessment will be, at a minimum, to ascertain —

(a) What information the intruder(s) may have accessed.

(b) What damage to security or disruption of operations may be caused by the intrusion.

(c) What protective measures should be implemented to mitigate the risk.

(5) All available information is provided to TRADOC CIO, tradociapm@monroe.army.mil, while the investigation and Force Protection assessment are conducted.

(6) Serious Incident Reports are completed as required by subparagraph d, above.

(7) The required Battle Damage Assessment and Intrusion Checklist are completed and submitted to RCERT after CCIU, ACERT, or RCERT approves rebuild of a compromised system.

**Paragraph 4-24, Information Assurance Vulnerability Management reporting process.**

Add subparagraph d:

d. *TRADOC implementation guidance.* Installations and activities shall complete actions required by IAVM messages as quickly as possible.

(1) Receipt of an Army IAVA is a CCIR item. TRADOC CIO will inform the TRADOC Commander of new Army IAVAs and explain the degree of difficulty in complying with each.

(2) TRADOC CIO will notify Installation Commanders of new Army IAVAs through TRADOC Operations Center taskings.

(3) Installation Commanders will ensure their IA and IT personnel understand that IAVM compliance is a top priority.

(4) Local extensions of IAVA suspenses are not authorized on installations with TRADOC Senior Mission Commanders. Installations may apply for a HQDA extension, if circumstances warrant. Installation Commanders will review all IAVA extension requests for their installations before they are submitted to HQDA. Extensions will not be requested unless the Installation Commander determines the affected systems are critical to the mission. Noncompliant systems, not covered by a HQDA extension or managed by an Army PM or non-Army equivalent, will be disconnected from all networks.

(5) Failure to complete required actions by an IAVA suspense date is a CCIR item.

(a) Installation Commanders will inform the TRADOC Commander via Spot Report (SPOTREP) any time a noncompliant system on the installation is left on any DoD network after an IAVA suspense, whether or not the system is covered by an HQDA-approved extension. The SPOTREP must explain why the vulnerable system was not disconnected from the network. Systems that may not be patched until directed by an Army PM or non-Army equivalent are excluded from this requirement.

(b) Installation Commanders will initiate an investigation under the provisions of chapter 4, [AR 15-6](#), any time a noncompliant system is left on an Army network after an IAVA suspense. Systems covered by a HQDA-approved extension or managed by an Army PM or non-Army equivalent are exempt from this requirement. The purpose of the investigation will be, at a minimum, to ascertain the cause(s) of noncompliance (human failure, systemic breakdown, etc.) and to determine appropriate corrective action.

(6) Installation Commanders; Commander, U.S. Army Accessions Command; Commandant, U.S. Army Ordnance Munitions and Electronics Maintenance School; Commandant, U.S. Army Ordnance Mechanical Maintenance School; Director, U.S. Army Aeronautical Services Agency; and Director, U.S. Army Nuclear and Chemical Agency will ensure that their installation/activity IAVA compliance status is reported to HQ TRADOC weekly until the Asset & Vulnerability Tracking Resource database is fully operational and

**TRADOC Suppl 1 to AR 25-2**

provides a MACOM Force Protection view. E-mail status to TRADOC CIO, tradociapm@monroe.army.mil, before close of business every Wednesday. In addition, installations and activities will report IAVA statuses NLT noon on the day after their suspense if they were not reported as completed on the last weekly report.

(7) TRADOC CIO will report the IAVA status of each installation to the TRADOC Commander every Friday morning.

FOR THE COMMANDER:

OFFICIAL:

ANTHONY R. JONES  
Lieutenant General, U.S. Army  
Acting Commanding General



JANE F. MALISZEWSKI  
Colonel, GS  
Chief Information Officer