Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-1047

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

14 September 2010

Information Management

INFORMATION ASSURANCE

FOR THE COMMANDER:

OFFICIAL:

JOHN E. STERLING, JR.
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff

LUCIOUS B. MORTON
Colonel, GS
Deputy Chief of Staff, G-6

History. This publication is supplement 1 to Army Regulation 25-2, dated 23 March 2009.

Summary. This supplement provides policy and mandates procedures for implementing the Army Information Assurance Program within the United States Army Training and Doctrine Command (TRADOC).

Applicability. This supplement applies to all TRADOC activities.

Proponent and exception authority. The proponent of this supplement is the Deputy Chief of Staff, G-6. The proponent has the authority to approve exceptions or waivers to this supplement that are consistent with controlling laws and regulations.

Supplementation. Further supplementation is prohibited without prior approval from the Deputy Chief of Staff, G-6 (ATIM-IA), 84 Patch Road, Fort Monroe, Virginia 23651-1047.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G-6 (ATIM-IA), 84 Patch Road, Fort Monroe, Virginia 23651-1047.

*Supersedes TRADOC Supplement 1 to AR 25-2, dated 18 August 2005.

Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

Availability. This publication is available only on the TRADOC Homepage at http://www.tradoc.army.mil/tpubs/supplndx.htm.

Supplement Army Regulation 25-2, 23 March 2009, as follows-

Paragraph 1-5.j

At the end of this paragraph, add the following: "Violations of paragraphs 4-34.c and 4-34.d of this supplement (identified in bold print) are punitive. Military personnel violating these paragraphs may be subject to action under the UCMJ and/or adverse administrative action. Civilian employees who violate this policy may also be subject to adverse action or discipline in accordance with applicable laws and regulations. Commanders and supervisors are reminded to consider their full range of options for addressing any failure to abide by this policy and to dispose of the case at the lowest appropriate level of authority consistent with the gravity of the misconduct."

Paragraph 3-1, Personnel structure overview

At the end of this paragraph, add the following: "When IA personnel discover information during the course of their normal activity that indicates a violation of acceptable use or a possible criminal offense, they will immediately report the finding to the suspected violator’s immediate commander or staff principal/director, whichever is most appropriate. Specifically, IA personnel do not have the discretion and authority to simply warn suspected offenders without reporting to the appropriate command or supervisory authority. The commander (or staff principal/director) will ensure that all reported offenses are quickly and thoroughly investigated. The commander himself may conduct the preliminary inquiry or direct someone else to do so (that is, commander’s inquiry or an AR 15-6 Investigation). In serious or complex criminal cases, the commander should seek the assistance of law enforcement personnel. The commander or supervisor will consult with legal counsel concerning activities that appear merely to violate acceptable use. IA personnel will retain and provide information related to the matter to appropriate investigative personnel when required. (See AR 25-2, para 4-21 and 4-22 for further guidance on reporting responsibilities.)"

Paragraph 4-3.a.(7)

At the end of this paragraph, add the following: "CORs and the requiring activity will ensure that contractor personnel supporting IA functions are certified in accordance with DOD 8570.01-M. The COR and the requiring activity will ensure that all TRADOC contract instruments reflect this DOD requirement. As determined by the contracting officer, this certification requirement will be incorporated by reference and/or included in any performance work statement or statement of work. For existing contract instruments that lack this certification requirement, coordinate with the contracting officer to modify the contract in conjunction with the exercise of a contract option or as part of a separate contract modification action. Such contract action should occur as soon as is practicable. Any questions regarding this requirement may be addressed to the TRADOC G-6."

After paragraph 4-15.i, add:

j. Foreign officials will not be provided a .mil address unless they are certified to Army in an official capacity, such as a/an FLO, CPP, ESEP, STANREP, MPEP, or IMS.

After paragraph 4-20.f.(8), add:

(9) All e-mails that contain sensitive information, information protected by the Privacy Act of 1974, or information protected under the Health Insurance Portability and Accountability Act must be encrypted with an approved DOD PKI certificate. Sensitive information includes personally identifiable information (PII) and For Official Use Only (FOUO) information.

(10) All e-mails sent from an Army-owned system or account that contain an active (embedded) hyperlink (uniform resource locator web address or e-mail address) and/or attachment must be digitally signed with an approved DOD PKI certificate. This applies to e-mails originating on workstations physically connected to the network, virtually connected wireless devices (for example, two-way e-mail devices, personal digital assistants, etc.), and remote workstations (such as, connected using a virtual private network). Limited exceptions to this policy are addressed in Army's BBP on digitally signing e-mail (https://informationassurance.us.army.mil/bbp/index.php). Additionally, a digital signature should be used whenever e-mail is considered official business (constituting orders, promulgating policy, or committing resources).

After paragraph 4-21.d, add:

e. Commanders, commandants, and directors of TRADOC activities; deputy chiefs of general staff offices; and chiefs of special staff offices will ensure-

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

(2) All suspected and confirmed intrusions are reported to the TRADOC DCS, G-6, monr.tradociapm@us.army.mil, within 1 work day of discovery.

(3) Appropriate activity personnel conduct a thorough force protection (FP)/operational security (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.

(4) All available information is provided to TRADOC G-6, monr.tradociapm@us.army.mil, while the FP assessment is conducted.

(5) Serious incident reports are completed as required by subparagraph 4-21d, above.

After paragraph 4-24.c, add:

d. *TRADOC implementation guidance*. Activities that administer mission IS shall complete actions required by IAVM messages as quickly as possible. The leaders of these activities will ensure that their IA and IT personnel understand that IAVM compliance is a top priority.

After paragraph 4-25.e, add:

f. Commanders, commandants, and directors of TRADOC activities; deputy chiefs of general staff offices; and chiefs of special staff offices will ensure that all required information for their activity's assets is entered into Army's IAVM compliance reporting tool and updated as changes occur. For common-use systems, the supporting Network Enterprise Center (NEC – formerly known as DOIM) can import IAVM compliance and most other required information into the compliance reporting tool from their automated network management and/or scanning tools. The tenant activity is responsible for entering and updating the rest of the required information; in particular, activities must ensure that records are deleted from the compliance reporting tool for systems no longer in use. Activities that administer mission IS shall report these systems' status in the IAVM compliance reporting tool, unless the supporting NEC provides this service.

After paragraph 4-31.a, add:

(1) Users shall not access documents known to contain sensitive information on Army Knowledge Online or other web-based systems from EOISs.

(2) Outlook Web Access users shall not open messages or attachments known to contain sensitive information from EOISs, or download attachments known to contain sensitive information to EOISs.

After paragraph 4-32, add:

Section XI
Data-At-Rest (DAR) and Mobile IS Security

4-33. TRADOC DAR policy

All sensitive information stored on government-owned or -leased desktops, mobile devices, and removable storage media must be protected using an Army-approved DAR encryption solution. Sensitive information includes PII and FOUO information. The following procedures will be followed:

a. The whole-disk DAR solution included in Vista and newer Microsoft client operating systems should be enabled on Windows computers. Current Windows versions refer to this solution as BitLocker. Army has approved the use of other whole-disk DAR solutions, but activities should not expend funds to purchase these unless there is a requirement which BitLocker cannot meet.

b. If BitLocker or another Army-approved whole-disk DAR solution is not enabled on a Windows computer, each user of the computer is responsible for using Windows' Encrypting File System (EFS) to encrypt all of their files containing sensitive information on the computer's hard drive(s). Procedures are contained in Army's DAR Protection BBP (https://informationassurance.us.army.mil/bbp/BBP%20DAR%20VER%201%200.pdf).

c. Users are also responsible for using EFS or another approved DAR solutions to encrypt all sensitive information they save on removable media. Removable media that cannot be encrypted using an Army-approved DAR solution are prohibited from storing sensitive information.

d. IASOs shall ensure that users are trained on what and how to encrypt using EFS or another Army-approved DAR solution.

4-34. TRADOC mobile IS security policy

The following mandatory procedures will be followed to protect government-owned or -leased IT equipment (computers, removable media, and personal digital assistants) and the data stored on this equipment:

a. Employees will not remove IT equipment and/or sensitive information from the workplace, for travel or other purposes, without the approval of their supervisor.

b. Supervisors must ensure that sensitive information approved for removal from the workplace is not subject to unnecessary risks of loss or compromise.

c. When IT equipment is removed from the workplace:

(1) When transported in a privately-owned vehicle, government-owned vehicle, or rental vehicle, IT equipment must be locked in the trunk of the vehicle during stops or when the vehicle is otherwise unattended. If the vehicle has no trunk, the equipment must not be left in an unattended vehicle.

(2) IT equipment will be handcarried or under visual observation while traveling on public transportation (for example, airplane, train, bus, or similar conveyance). If the computer carrying case is too large to be carried on an airplane, the IT equipment will be removed from the case and handcarried onto the airplane.

(3) IT equipment will not be left in an unattended, unsecured personal residence where it could be stolen. If IT equipment is left unattended in the residence, all windows

and exterior doors must be locked or the equipment must be secured in a locked safe or cabinet or secured with a cable lock to an immovable object.

(4) IT equipment will not be left unsecured in a hotel room where it could easily be stolen. All windows and doors must be locked, and equipment must be secured in a locked safe or cabinet or secured with a cable lock to an immovable object.

d. Laptops, portable notebooks, tablet PCs, and similar systems will not be left unattended and unsecured in the workplace. If not under direct observation or control, these devices must be in a locked office, locked in an appropriate container (such as, safe, closet, cabinet), or secured to an immovable object with a cable lock. If authorized to use a mobile IS at a TDY location, the responsible individual will secure this IS to the same standard as at home station.

e. Supervisors and users will consider methods to reduce the amount of sensitive information stored on removable media. Such methods include limiting the use of removable media, storing files on AKO, or using encrypted e-mail.

f. In the event of lost/stolen IT equipment on post, users must immediately contact the Military Police to report the loss. If the loss occurs off post, contact the local police. Users will also report the loss to their IASO. If the lost or stolen IT equipment contained PII, then supervisors and users must follow reporting guidelines in TRADOC Regulation 1-8, paragraph 2-2 and appendix D.

g. Financial liability for the loss or theft of IT equipment shall be evaluated in accordance with AR 735-5. Failure to follow this policy or other guidance on IT security may constitute negligence and could subject the violator to personal financial liability.

h. Mobile IS approved for travel will be labeled, using local procedures, to indicate that they are approved for travel. Place labels inside the lid of laptops, not on the outside, to avoid advertising these devices as government systems containing sensitive information. If the IS is protected by an approved DAR solution, this shall be stated on the label.

After paragraph 5-10, add:

5-11. TRADOC C&A implementation guidance

All ISs must be certified and accredited in accordance with the DIACAP. In addition to the procedures outlined in DOD Instruction 8510.01 and AR 25-2, TRADOC SO will complete the following:

a. Inform TRADOC G-6, monr.tradociapm@us.army.mil, that he/she is initiating C&A of an IS. Once this initial contact has been made, TRADOC G-6 will inform the SO where to post the C&A documentation for the IS.

b. Identify an individual in the rank of general officer, senior executive service member, or equivalent to be the IS’s DAA. The SO must brief the individual on DAA responsibilities and receive approval from the candidate to nominate him/her as the DAA. Once the individual has agreed to serve as the DAA, the SO will e-mail the candidate's name and duty position to TRADOC G-6 IAPM, monr.tradociapm@us.army.mil. TRADOC G-6 will submit the DAA nomination to DA CIO/G-6. After verifying the credentials of the nominee, DA CIO/G-6 will send this individual a digitally-signed e-mail appointing him/her as a DAA. The DAA must complete the online DAA training at https://iatraining.us.army.mil/_usermgmt/login.htm within 30 days of appointment. After completing the DAA training, the DAA is required to send a copy of his/her certificate of training to the TRADOC G-6 IAPM at monr.tradociapm@us.army.mil.

c. Ensure that properly trained and certified personnel are appointed in writing to fill the following key C&A positions:

(1) IAM. Must be appointed in writing by the DAA.

(2) System administrators. Must be appointed in writing by the SO or IAM.

d. Register the system in the Army Portfolio Management Solution (APMS), https://apms.us.army.mil/prosight, as required by CON and FISMA requirements. If the SO has not completed the required training for APMS, they will need to contact the TRADOC G-6 at monr.tradociapm@us.army.mil to coordinate this training.

e. Define or review the accreditation boundary for equipment and networks.

f. Determine if system diagrams exist or need to be created. Diagrams should adhere to the Department of Defense Architecture Framework, as defined at http://www.defenselink.mil/cio-nii/cio/earch.shtml. This framework is also required when the SO submits a request for a CON.

g. Determine if an Interim Authority to Operate or Interim Authority to Test is needed while C&A is in progress. For definitions and descriptions of these, refer to Army BBP 06-DC-M-0002 C&A.

h. Determine mission assurance category and confidentiality level with members of the DIACAP team.

i. Submit the completed system identification profile (SIP) to TRADOC G-6, monr.tradociapm@us.army.mil, for review. After any required changes have been made, the SO will have to register the IS in the Army C&A Tracking Database (C&A TdB), found at https://armydiacaptdb.arl.army.mil/drupal/caclogin.php. After the SO completes the registration and uploads the IS SIP in the C&A TdB, the OIA&C will appoint a Certification Authority Representative.

j. SO will coordinate with the TRADOC G-6 to upload all C&A documentation to a portal developed as a repository for all TRADOC IS.

k. Draft the DIACAP Implementation Plan (DIP).

l. Select an organization from Army's approved ACA list, found at OIA&C's knowledge center on AKO, https://www.us.army.mil/suite/files/4307492, to conduct the required security test & evaluation (ST&E). Per Army BBP 06-DC-M-005, the ST&E has to be performed by a third party not affiliated with the IS. The SO should request quotes from three or more ACA organizations and then select the one that best supports his/her program requirements, including cost and scheduling. TRADOC G-6 will provide information to assist the SO in choosing an ACA.

m. Develop a timeline for testing and certification completion based on available documentation, mission-need, and ACA testing schedule. Reconcile budgets to support C&A process, including manpower costs, equipment purchase or update, and ACA testing.

n. Ensure the following are accomplished in preparation for the ACA's ST&E:

(1) All systems are patched and configured according to DISA and Army guidelines.

(2) Waivers are documented and current.

(3) MOAs or MOUs are in place with the supporting NEC. If a COOP site has been identified, then MOAs or MOUs must also be established with the activity responsible for the COOP site.

(4) All DIACAP documentation is available for review.

(5) DIACAP team personnel are available to be interviewed by the ACA team.

o. Submit updated C&A documentation to TRADOC G-6, monr.tradociapm@us.army.mil, after completion of ST&E. TRADOC G-6 IA Directorate will review the documentation for completeness and provide feedback to the SO. If any corrections are necessary, TRADOC G-6 will return the package, with comments, to the SO for updates. After corrections are made, TRADOC G-6 will forward the completed package to DA CIO/G-6 for final review and approval. The ACA will prepare a scorecard and an IATO or ATO recommendation based on the results of the ST&E.

p. SO are required to develop a POA&M for documenting all findings from the ACA ST&E. If an IATO is recommended by the ACA, the SO must complete the following:

(1) Work to resolve all findings, and update the POA&M as findings are completed. Provide updated copies to the assigned CAR and TRADOC G-6.

(2) Obtain a waiver from the assigned DAA addressing any IA controls that cannot be implemented on the system. Provide a copy to the assigned CAR and TRADOC G-6.

q. Revalidate accreditation documentation and controls annually and provide a written statement or digitally signed e-mail to the TRADOC G-6, monr.tradociapm@us.army.mil, that either confirms the effectiveness of assigned IA controls and their implementation or recommends changes or improvements. If the SO recommends changes or improvements, the DIACAP team will implement them and then resubmit the POA&M. After all required changes and improvements are completed, the SO will:

(1) Provide a revalidation statement to HQDA and TRADOC G-6 by the annual certification date (for example, if the IS was originally accredited on 8 Oct 09, the first review must be completed no later than 7 Oct 10).

(2) Report revalidation results in APMS to maintain FISMA compliance.

r. Obtain a CON before they connect hardware or software to the LandWarNet. To obtain a CON, the SO must complete the appropriate Networthiness Checklist (Application, System, or Interim Authority to Test), which can be found at https://www.us.army.mil/suite/grouppage/16220. Once the checklist has been completed, the SO will submit it to TRADOC G-6, monr.tradociapm@us.army.mil, for review. TRADOC G-6, IA Directorate, will review all documentation for completeness and accuracy and provide feedback to the SO. If any corrections are necessary, TRADOC G-6 will return the Networthiness Checklist, with comments, to the SO for updates. Once the updates have been made, the SO will submit the completed Networthiness Checklist, with supporting DIACAP documentation, to their supporting NEC. After the installation IAM and NEC approve the use of the IS or application, the SO will submit the documentation mentioned above to the NETCOM Networthiness Team at Army.Networthiness@us.army.mil for final review and approval. SOs will courtesy copy the TRADOC G-6 at monr.tradociapm@us.army.mil when they submit documentation to NETCOM.

In Glossary; Section I, Abbreviations, add:

APMS	Army Portfolio Management Solution
DAR	Data-At-Rest
DIP	DIACAP Implementation Plan
EFS	Encrypting File System
FOUO	for official use only
FP	force protection
IMS	international military student
NEC	Network Enterprise Center
OPSEC	operational security
PII	personally identifiable information
PKI	public key infrastructure
SIP	system identification profile
ST&E	security test & evaluation
TdB	tracking database

In Glossary; Section II, Terms, add:

Mobile computing devices (MCD)

Laptops, portable notebooks, tablet-PCs, and similar systems; and removable/external storage devices such as thumbdrives, external hard drives, CDs, DVDs, or floppy diskettes.

Mobile information system (MIS)
Laptops, portable notebooks, tablet-PCs, and similar systems; and removable/external storage devices such as thumbdrives, external hard drives, CDs, DVDs, or floppy diskettes.