

MEMORANDUM FOR RECORD

SUBJECT: Army Addendum to DOD Information Assurance (IA) User Awareness training.

DOD References:

- DoDD 8570-01 Information Assurance, Training, Certification and Workforce Management, 23 Apr 07 (<http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>)
- DoD 8570.01-M Information Assurance Workforce Improvement Program, 15 May 08 (<http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>)
- DoDD 8500.01E Information Assurance, 23 Apr 07 (<http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>)
- DoDI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 Nov 07 (<http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>)
- DoDI 8500.2 Information Assurance (IA) Implementation, 6 Feb 03 (<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>)

Joint References:

- JTF-GNO CTO 07-015 Revision 1, Public Key Infrastructure (PKI) Implementation, Phase 2, 7 Apr 08 (https://www.cert.mil/operations/cto/2008/CTO_07_15/CTO_PKI_Phase2_rev_1_7APR08.doc) (CAC Enabled)

Army References:

- PR-M-0002 Information Assurance (IA) Training and Certification, 30 Nov 09 (https://atc.us.army.mil/iastar/Training_BBP.pdf) (CAC Enabled)
- AR 25-1 Army Knowledge Management and Information Technology Management, 4 Dec 08 (http://www.army.mil/usapa/epubs/pdf/r25_1.pdf)
- AR 25-2 Information Assurance, 23 Mar 09 (http://www.army.mil/usapa/epubs/pdf/r25_2.pdf)
- Army Password Standards, Ver 2.5, 1 May 08 (CAC Enabled) (https://informationassurance.us.army.mil/bbp/army_password_standards.pdf)
- Army Transition Plan for Training and Certification Tracking System, 17 Oct 07 (https://atc.us.army.mil/iastar/army_training_and_certification_transition_plan.pdf)
- Army Information Assurance Virtual Training (CAC Enabled) (https://iatraining.us.army.mil/_p2g/header2gen.php)

1. In addition of the DOD IA User Awareness training, the following guidance is provided to include specific Army policy considerations.

2. DoDD 8570-01 Information Assurance, Training, Certification and Workforce Management

Establishes policy and assigns responsibilities for DoD IA training, certification, and workforce management. Authorizes the publication of DoD 8570.1-M

3. DoD 8570.01-M Information Assurance Workforce Improvement Program

This Manual: implements DoD Directive 8570.1 and provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance functions within the DoD workforce supporting the DoD Global Information Grid per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation and vulnerability assessment will be published as changes to this Manual. It establishes IA workforce oversight and management reporting requirements. This manual establishes IA workforce and management reporting requirements.

4. DoDD 8500.01E Information Assurance

This Directive establishes policy and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. It designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

5. DoDI DoD Information Assurance Certification and Accreditation Process (DIACAP)

This Instruction establishes the DIACAP for authorizing the operation of DoD ISs. It establishes or continues the following positions, panels, and working groups to implement the DIACAP: the Senior Information Assurance Officer, the Principal Accrediting Authority, the Defense Information Systems Network/Global Information Grid Flag Panel, the IA Senior Leadership, the Defense IA Security Accreditation Working Group, and the DIACAP Technical Advisory Group. It establishes a Certification and Accreditation process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications. This Instruction prescribes the DIACAP to satisfy the requirements of Reference (a) and requires the DoD to meet or exceed the standards required by the Office of Management and Budget and the Secretary of Commerce.

6. DoDI 8500.2 Information Assurance (IA) Implementation

This Instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD ISs and networks.

7. 05-PR-M-0002 Information Assurance (IA) Training and Certification

The IA workforce focuses on the operation and management of IA capabilities for Department of Defense systems and networks. IA ensures that adequate security measures and established IA policies and procedures are applied to all ISs and networks. The IA workforce includes all privileged users and IA managers who perform any of the responsibilities or functions. These responsibilities include: developing, testing, deploying, operating, administering, troubleshooting, managing, and retiring DoD ISs. To support the warfighter in a highly effective and professional manner, the Army must ensure that appropriate levels of IA awareness, training, education, certification, and workforce management are provided to the IA workforce and IS users that commensurate with their respective responsibilities.

The IA training audience includes military, civilian, foreign nationals and contractor personnel in Deployed and Generating Forces organizations. In addition to being able to demonstrate the required level of technical and/or managerial skills and experience, it is DoD policy (DoDD 8570.1) that “the IA workforce knowledge and skills be verified through standard certification testing.” Consequently, Army IA personnel must attain and maintain Information Technology /IA certifications appropriate for the technical and/or managerial requirements of their position. In some cases, this will include passing one or more certification exams. IA Workforce personnel in Technical and Management Level positions must complete eighty hours of sustainment training biannually or as required to maintain certification status, whichever is greater.

8. AR 25-1 Army Knowledge Management and Information Technology

This regulation establishes the policies and assigns responsibilities for the management of information resources and information technology (IT). It applies to IT contained in command and control (C2) systems, intelligence systems, business systems, and (except as noted) national security systems developed or purchased by the Department of Army. It addresses the application of knowledge management concepts and systems across the Army, the management of information as an Army resource, the technology supporting information requirements, and the resources supporting command, control, communications, and computers (C4)/IT.

9. AR 25-2 Information Assurance

The AR 25-2 provides IA policy, mandates, roles, and responsibilities, and procedures for implementing Army Information Assurance Program, consistent with today’s technological advancements for achieving acceptable levels of security in engineering, implementation, operation, and maintenance for ISs connecting to or crossing any U.S. Army managed network.

A. According to AR 25-2, a general system user is responsible to:

1. Comply with command’s Acceptable Use Policy (AUP) for government owned ISs and sign AUP prior to or upon account activation.
2. Obtain prior approval for the use of any media (USB, CD-ROM, floppy disk).
3. Scan all files, attachments, and media with an approved and installed Anti-virus (AV) product before opening a file or attachment or introducing media into the IS.
4. Not disclose their individual account password or pass-phrase authenticators.
5. Invoke password-protected screen locks on your workstation after not more than 15 minutes on non-use or activity.
6. Logoff ISs at the end of each workday.
7. Access only that data, control information, SW, HW and firmware for which the user is authorized access.
8. Protect information not authorized to be released for public disclosure.
9. Assume only authorized roles and privileges as assigned.
10. Prevent sharing their personally assigned e-mail accounts.
11. Prohibit auto-forwarding of official e-mail to non-official accounts or devices.

B. AR 25-2 includes a list of specific prohibited activities that users must be aware of. Some of these include:

1. Use of ISs for unlawful or unauthorized activities, such as filesharing of media, data, or other content that is protected by the Federal or State Law, including copyright or other intellectual property statutes.
2. Installing software, configuration of an IS or connecting and ISs to a distributed computing environment (including wireless access points)
3. Modification of the IS or software, use of the IS for any other manner other than its intended purpose, or adding user-configurable or unauthorized software, such as but not limited to commercial instant messaging (IM), commercial Internet chat or collaborative environments, or peer-to-peer client applications.
4. Any attempt to strain, test, circumvent, or bypass network or IS security mechanisms or to perform network keystroke monitoring.
5. Physical relocation or changes to configuration or network connectivity of IS equipment.
6. Installation of non-Government-owned computing systems or devices without prior authorization of the appointed DAA including but not limited to USB devices, external media, personal or contractor-owned laptops, and MCDs
7. Sharing personal accounts and authenticators (passwords or PINs) or permitting the use of remote access capabilities through Government provided resources with any unauthorized individual
8. Disabling or removing security or protective software and other mechanisms and their associated logs from IS.

C. As a minimum, annual refresher training must be completed by a user to continue to operate on the IS.

D. Personnel requiring access to ISs to fulfill their duties must possess the required favorable security investigation, security clearance, or formal access approval, and fulfill any need-to-know requirements.

E. Army Information Assurance Program (AIAP) is a unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by ISs, and is established to consolidate and focus Army efforts in securing that information, including its association systems and resources, in increase the level of trust information and the originating source.

F. IA Best Business Practices (BBPs) are the best ideas, concepts, and methodologies acquired from industry and Army resources that allow rapid transitional implementation of IA initiatives to integrate, use, improve, or modify technological or procedural changes as required by policy. BBPs are located at <https://informationassurance.us.army.mil>.

G. Defense in Depth (DiD) encompasses a physical and logical structure that requires a layering of security policies, procedures, and technology mechanisms to protect network resources, from the desktop to the enterprise, within and across the enterprise architecture. DiD elements focus on three areas: people, operations and defense of the environment.

H. IA Personnel Structure. Users need to understand their role in IA. This includes protecting their password from compromise, reporting anything suspicious regarding unexpected

or unusual behavior on a computer system. Users should report problems to their unit Information Assurance Security Officer (IASO). The IASO is responsible for enforcing policy, guidance and training requirements, such as providing annual user awareness training, as well as implementing Information Assurance Vulnerability Management (IAVM) in the unit/organization.

I. Instant Messaging (IM) is a real time communications service that may include capabilities such as sending text notes to others online; custom chat rooms; shared web links; the ability to look at images on some else's computer; the ability to hear sounds someone else is playing or play sounds for others to hear; sharing files through direct send; audio conversations; and streaming content such as real-time or near-real time news or stock quotes. Many commercial entities, e.g., AOL, Microsoft, Yahoo, offer instant messaging as an unregulated Internet service.

Individual end user subscriptions to any non-DoD IM service such as AOL or Microsoft from a computer on a DoD network is prohibited.

This does not include officially authorized subscriptions to non-DoD services for special circumstances, e.g., quality of life in theater (i.e. deployed and Commanders approval), provided adequate measures are taken to protect DoD networks against external penetration or denial of service via IM.

Instant messaging can be provided as a DoD service by a DoD enclave or AIS application. Instant messaging services under the configuration control of DoD may be used for official DoD business if compliant with IA policies for ports and protocols management, mobile code, etc., and approved for use by a DAA. IT program managers considering outsourcing of IM services for the conduct of official DoD business must ensure that DoD information (i.e., user identifiers and the message traffic) is protected at the sensitive level, and that DoD networks are protected against external penetration or denial of service via IM. Sensitive level implies encryption or encrypted sessions.

AKO portal is the Army instant message server and is the only IM currently authorized for use and installation in Army organizations. Sametime, while never addressed specifically in a policy statement, would meet the protection requirements for those environment that use it since it is a specifically targeted application to support Lotus, as long as the same considerations are taken as with IM, i.e. no commercial connections, no user installations, or external connections etc. No other IM product would be approved at this time since the capability exists, an authorized product is available, and AKO is currently the only authorized site.

10. Army Password Standards BBP

1. All system or system-level passwords and privileged-level accounts (e.g., root, enable, admin, administration accounts, etc.) will be a minimum of 15-character case-sensitive password changed every 60 days (IAW JTF-GNO CTO).
2. All user-level, user-generated passwords (e.g., email, web, desktop computer, etc.) will change to a 14-character (or greater) case-sensitive password changed every 60 days.

3. Password history will be set to a minimum of 10.

4. Set the Observation Window for Account lockout settings to no more than 60 minutes. Set the LockoutDuration setting (also known in Group Policy as the Account lockout duration setting) to 0 and the LockoutThreshold setting (also known in Group Policy as the Account lockout threshold setting) to 3. This allows no more than two unsuccessful logon attempts within a 60 minute period and requires a system administrator to unlock the account.

5. When supported, enable that system capability to notify the user of last successful and unsuccessful logon time and date. Users will notify administrative and security personnel when discrepancies are identified.

6. The password will be a mix of uppercase letters, lowercase letters, numbers, and special characters with a minimum of characters as follows:

a. Contains at least 2 uppercase characters: A, B, C etc.

b. Contains at least 2 lowercase characters: a, b, c, etc.

c. Contains at least 2 numbers: 1,2,3,4,5,6,7,8,9,0

d. Contains at least 2 special characters:

! @ # \$ % ^ & * () _ + | ~ - = \ ` { } [] : " ; ' < > ? , . /

7. Passwords will not have the following characteristics:

a. Is a word found in any dictionary, thesaurus, or list (English or foreign)

b. Is any common usage word or reference such as:

(I) Names of family, pets, friends, co-workers, fantasy characters, etc.

(II) Computer terms and names, commands, sites, companies, hardware, software.

(III) Common words such as; "sanjose", "sanfran" or other derivative.

(IV) Birthdays, addresses, phone numbers, or other personal information.

(V) Word or number patterns like; aaabbb, qwerty, mypassword, abcde12345.

(VI) Any of the above spelled backwards.

(VII) Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

(VIII) Social security numbers (SSNs).

(IX) USERID

(X) Military slang, acronyms, or descriptors or call signs.

(XI) System identification.

8. The use of eight character passwords are authorized when:

a. The password generated is a purely **random-generated** authenticator from the complete alpha/numeric and special character sets and no user-configured passwords can replace, be generated, or accepted in lieu of the generated password. (For example: Credentialing system issues randomly generated authenticator AND enforce use of that authenticator to network resources.)

b. Access to private applications is conducted over an approved 128-bit encrypted session between systems, and the application does not enforce local user access credentialing to a local network resources. (For example: User accesses local LAN connected system through traditional access procedures then accesses a web portal application over an SSL connection; the web portal password may be 8 characters.)

TACTICAL SYSTEMS NOTE: Deployed/tactical systems with limited data input capabilities will also implement these measures except in those cases where implementation of this guidance is operationally impractical or adversely impose risk of safety-of-use because of the function and design of the system. Deviations from password standards in these cases will be addressed in the accreditation documentation as well as in the approval to operate memorandum signed by the DAA. Only DAAs recognized in writing by the Army CIO/G-6 may approve these case-by-case deviations.

11. Army Training and Certification Transition Plan

This plan is to provide guidance to the IA community on how to transition their training and certification status and information into the new Army Training and Certification Tracking System. This system will enable managers and supervisors a snapshot of their organization training and certification status verified by/from an authoritative source.

12. Army Memorandum on Inappropriate Use of E-mail. (AR 25-1)

Inappropriate use of E-mail systems may be a basis for consideration of disciplinary action against soldiers and civilian employees. Users should use e-mail resources responsibly and abide by normal standards of professional and personal courtesy and conduct at all times. Systems will NOT be used in a way that would interfere with official duties, undermine readiness, reflect adversely on DoD or the Army (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling via e-mail; and other uses that are incompatible with public service), or further any unlawful activity of personal commercial purposes.

Users of Army E-mail services will not use these services in a manner that overburdens Army telecommunications systems. Users should NOT use e-mail services to:

- (1) send e-mail chain letters;
- (2) "spam," that is, exploiting listservers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail;
- (3) broadcast unnecessary advertisements of Army services;
- (4) "letter-bomb," that is, to send the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail;
- (5) broadcast e-mail messages of daily quotations, jokes, or other similar transmissions;
- (6) broadcast unsubstantiated virus warnings from sources other than systems administrators; and,
- (7) directing messages to large audiences and sending repeats of the same messages as "reminders."

13. Army Policy on the Use of Web-Based or Internet Service Provider (ISP) E-mail Accounts for Official Army Business

Federal Government sponsored E-Mail accounts are for Official Army business. Using non-approved ISP or web based systems as alternative E-Mail addresses for official Army business is prohibited. Army Employees will not use unapproved accounts (such as Hotmail or Yahoo mail) for Official Army business unless specifically authorized to do so by their DOIM. Army employees shall not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices. Army employees should exercise

ATZH-LCS-IAD

SUBJECT: Army Addendum to DOD IA User Awareness Training

extreme care when transmitting any sensitive information, or other valued data. Information transmitted over an open network (such as through web based or ISP unsecure E-Mail) may be accessible to anyone else on the network.

(<http://www.army.mil/ciog6/policy/docs/WebBasedPolicy.txt>)

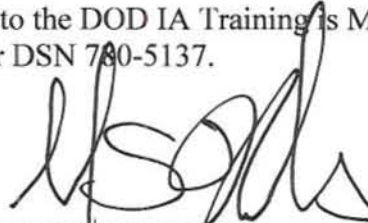
14. Army Data-at-rest (DAR) Protection Strategy

Mobile information systems (IS) require DAR remediation procedures to protect Army information. Laptops designated for travel support must be identified and labeled as appropriate. Understanding and compliance with reporting procedures to notify leadership of loss of protected IS through appropriate privacy and incident response channels. Organizations should leverage existing MS Encrypting File System (EFS) capabilities with Active Directory (AD) management structure to enable file encryption through a centrally managed EFS certificate issuance. Information should be encrypted while stored on official IS.

(<https://informationassurance.us.army.mil/bbp/BBP%20DAR%20VER%201%200.pdf>)

(<https://informationassurance.us.army.mil/dar/FAQ%20Interpreting%20DoD%20Policy%20Memo%20for%20Data%20At%20Rest%2004Sep07%20v1%20Final.pdf>)

15. Point of contact for this Army Addendum to the DOD IA Training is Mr. Joey Gaspard, joey.gaspard@us.army.mil, (706) 791-5137 or DSN 780-5137.



AUBREY S. HINDS

MAJ, LG (53A)

Chief, Information Assurance Division