

12 July 2006

Information Management: Management of Subdisciplines

Army Information Assurance

For the Commanding General:

WILLIAM G. KIDD
Colonel, GS
Chief of Staff

OFFICIAL:



F. W. MORRIS
Chief, Publications and
Record Management

Summary. This supplement prescribes policy and procedures for classified and unclassified information assurance in the Army in Korea.

Applicability. This supplement applies to commands and units in the Korean theater that have accounts on or connectivity to Army in Korea information networks.

Supplementation. Organizations will not supplement this supplement without Regional Chief Information Officer, Republic of Korea Region (RCIO-K) approval.

Forms. Army in Korea (AK) forms are available at www.usfk.mil.

Records Management. Records created as a result of processes prescribed by this supplement must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System (ARIMS) website at <https://www.arims.army.mil>.

Suggested Improvements. The proponent of this supplement is the RCIO-K. Users may suggest improvements to this supplement by sending e-mail to rciokpubs@korea.army.mil.

Distribution. Electronic Media Only (EMO).

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

Contents. Add the following to the appendix list:

D. Consolidated IA Certification Requirements

Contents. Add the following to the table list:

Table 3-1: Required IA Positions in the Army in Korea

Table D-1: Information Assurance Training and Certification Requirements for the Army in Korea

After paragraph 2-8, Commander, 1st Information Operations Command (LAND). Add paragraph 2-8.1 as follows:

2-8.1. Regional Computer Emergency Response Team – Korea (RCERT-K)

The RCERT-K will—

- a. Identify and handle computer incidents and intrusions involving the Army in Korea LandWarNet (Unclas) and LandWarNet (Class) infrastructure, and recommend protective measures.
- b. Integrate Computer Network Defense (CND) support of information operations (IO) in coordination with the 1st Signal Brigade, Eighth U.S. Army CIO/G6, and (Eighth Army), RCIO-K.
- c. Provide technical assistance when requested to the Military Intelligence Group for law-enforcement and counterintelligence activities involving Army in Korea networks.
- d. Provide any finding of unusual/suspicious and unauthorized activities to DOIMs for follow-up actions.
- e. Perform necessary scanning on networks when requested by proper authority.
- f. When requested by commanders, perform Computer Defense Assistance Program (CDAP) activities and provide briefings on findings and ways to improve computer security.
- g. Provide recommendations for preventive measures or response activities as necessary.
- h. Identify critical points of failure and other potential vulnerabilities in the Army in Korea communications infrastructure and recommend protective measures.
- i. As a non-voting member for CCB, ensure IA is properly implemented.

After paragraph 2--9, Commanding General, Network Enterprise Technology Command/9th Army Signal Command. Add paragraph 2-9.1 and 2-9.1.1 as follows:

2-9.1. 1st Signal Brigade

1st Signal Brigade will—

- a. Operate, manage, monitor, administer, and defend the Army in Korea portion of the LandWarNet.
- b. With the assistance of the Army in Korea IAPM, provide IA support, advice, and assistance to Army in Korea customers through Theater Network Operations and Security Center (TNOSC) Korea and DOIM IAMs
- c. Provide guidance and priorities to the RCERT-K concerning IA/CND support for the Army in Korea.
- d. Establish and maintain Configuration Control Board (CCB) for LandWarNet in Korea.

2-9.1.1 TNOSC Korea

TNOSC Korea will --

- a. Perform configuration and patch management for all Top Layer Architecture (TLA) network components and systems to include Enterprise Managed systems and solutions.
- b. In coordination with the RCERT-K, Eighth Army CIO/G6, and RCIO-K, establishes tactics, techniques, and procedures (TTP) for IA/CND activities for inclusion in "Network Operations" TTP.
- c. Maintain Active Directory (AD) and E-mail system for Army in Korea networks.
- d. Ensure that all critical assets (TLA - routers, firewalls, proxies, cache, and IDS/IPS) are IAVA compliant and fully protected. Vulnerability assessments must be performed on a monthly basis of these crucial assets. Coordinate with supporting RCERT to conduct independent vulnerability assessment and/or minimal (non-intrusive) penetration testing (verification of access controls).
- e. Coordinate with RCIO-K and DOIMs on taskings from higher authority and provide timely input.
- f. Perform software evaluation upon request for distribution and installation in the Army in Korea networks.
- g. As a voting member for CCB, ensure IA is properly implemented.
- h. Provide the MACOM and COCOM tailored views to a Network Common Operating Picture (NETCOP) and/or Information Assurance Situational Awareness. These views will provide the Commander with the current operational status of crucial assets.
- i. Participate with law enforcement organizations in analyses and studies concerning foreign intelligence threats and criminal or operational vulnerabilities against which IA countermeasures should be directed.
- j. Install and maintain anti-virus and patch management servers to automatically update all systems in the Army in Korea networks.
- k. Provide technical review/input for all standard network configurations such as Firewall Exception Request (FER) or Trusted Host Request (THR).

Paragraph 2-15, Commanders, Directors, and Managers. Add subparagraphs h through n as follows:

- h. Ensure all personnel read and sign Acceptable User Policy (AUP) prior to access government system.
- i. If serving as a DAA, appoint an IAM and a Certification Authority (CA).
- j. Ensure all IA personnel are trained and certified according to appendix D.
- k. Ensure all users take Computer User training and annual refresher.
- l. Ensure all users take and pass the Computer-User Test.
- m. Take appropriate actions (investigate, retrain, or punish) on personnel suspected of engaging in prohibited computer-network activities and take protective measures on unauthorized activities.
- n. Remain informed at all times of their unit's IA posture and take appropriate actions to mitigate risks to information and ISs under their control. Commanders and directors will request help from their DAA when additional IA policy or technical advice and assistance is needed.

Paragraph 2-16, Garrison commanders. Add subparagraph i as follows:

- i. Coordinate with RCIO-K and DOIMs on configuration management and operation of the installation network.

Paragraph 3-2, Information Assurance Personnel Structure. Add the following table:

Table 3-1 lists the minimum required IA positions in the Army in Korea and the unit and organization levels at which the positions must exist and be filled by qualified personnel. Individuals filling these positions must be appointed. Paragraph 4-3 and appendix D provide training and certification requirements

Table 3-1 Required IA Positions in the Army in Korea (note)		
Echelon	Position Title	Foreign National May Fill
Battalion or equivalent units; staff offices headed by a Lieutenant Colonel or equivalent	Information assurance security officer (IT-I or IT-II)	Not allowed if the position is IT-I; conditionally and temporarily allowed if the position is IT-II (table 4-3).
Brigade or equivalent units	Information assurance manager (IT-I) (each DAA will appoint an IAM)	Not allowed.
As determined by the unit or organization G6 or equivalent	System or network administrator (IT-I or IT-II)	Conditionally allowed. Conditions differ based on whether the position is IT-I or IT-II (tables 4-2 and 4-3).
1 st Signal Brigade only	Information assurance network manager (IANM) (IT-I)	Not allowed.
Major Subordinate Command	Information assurance manager (IT-I) (each DAA will appoint an IAM)	Not allowed.
Eighth U.S. Army	Information assurance program manager (IAPM) (IT-1) (Eighth Army CIO/G6 will appoint the IAPM)	Not allowed.
NOTE: Paragraph 4-14 provides the definitions of IT-I and IT-II.		

After paragraph 3-2.a NETCOM Regional Chief Information Officer (RCIO). Add paragraph 3-2.a.1 as follows:

a.1 RCIO – Korea

RCIO - Korea will –

- (1) Oversee the Army in Korea IA program.
- (2) Be Designated Approving Authority for LandWarNet (Class) in Korea.
- (3) Appoint the Army in Korea Information Assurance Program Manager (IAPM).
- (4) Appoint the Protective Distribution System (PDS) Certifying Agents.
- (5) Provide advice and assistance to organizations' DAAs in the Army in Korea LandWarNet regarding the C&A process.
- (6) Provide comprehensive planning and programming of Army in Korea IA requirements for management decision packages (MDEPs) MS4X, and promote the development of Army in Korea IA resources through the planning and budgeting process.
- (7) Oversee the Army in Korea Public Key Infrastructure (PKI) Program and follow NETCOM guidance for overall PKI implementation in Army in Korea.
- (8) Coordinate with TNOSC and DOIMs to ensure IA programs are implemented across all AISs connecting to Army in Korea networks within their scope of responsibility, and ensure that all networks are run in accordance with applicable regulations.
- (9) Oversee and manage the Army in Korea IAVM Program, including A&VTR reporting requirements.
- (10) Develop and manage Army in Korea IA Training Program.

(11) Serve as a voting member of the Configuration Control Board.

Paragraph 3-2.b Information Assurance Program Manager (IAPM). Add subparagraph (22) as follows:

(22) Provide advice and assistance on the construction of protected distribution systems and endorse PDS certification by designated Certifying Agents.

Paragraph 3-2.d Information Assurance Manager (IAM). Add subparagraphs (21) through (27) as follows:

(21) Tenant IAM will be appointed by the DAA for the organization.

(22) Tenant IASO/IAM will work with Area IAM for all IA issues.

(23) Area DOIM IAM will review all C&A packages and ensure all packages are properly formatted and documented.

(24) Area DOIM IAM can be appointed as the CA when an independent agency is not available to participate in the C&A process.

(25) Ensure the DAA is trained on his or her responsibilities.

(26) Ensure IA requirements are incorporated in all contract performance work statements (PWSs) for IT services or equipment.

(27) Develop and enter the commander's IA and COMSEC requirements (MS4X (Computer Security) and MX5T (Communications Security (COMSEC)) equipment) into the Information Systems Security Program (ISSP).

Paragraph 3-2.f Information Assurance Security Officer (IASO). Add subparagraph (14) as follows:

(14) As a minimum, be appointed at all battalion or equivalent level units and staff offices headed by a Lieutenant Colonel or equivalent.

Paragraph 3-3.a System or network administrators. Add subparagraphs (23) through (29) as follows:

(23) Ensure all systems and users comply with Army in Korea Information Assurance supplement and PAM.

(24) Ensure all users read and sign Army in Korea Acceptable User Policy, and take and pass Computer User Test.

(25) Ensure that all systems connected to the Army in Korea LandWarNet are configured with the Army standard configuration baseline.

(26) Not establish any unauthorized VPN connectivity or remote access connection to bypass the Army in Korea LandWarNet.

(27) Not attempt to extend the existing cable-based network by installing wireless technology unless approved by the DAA IAW paragraph 4-29 of this regulation.

(28) Ensure all networked computers are pointed to antivirus and software update servers managed by TNOSC.

(29) Ensure vulnerability scans are conducted on computers that belong to the organization periodically.

Paragraph 3-3.c.(1) User responsibilities. Add subparagraphs (p) through (s) as follows:

(p) All LandWarNet users in the Army in Korea will read Acceptable Use Policy (AUP) and accept obligation by signing the document, and a copy of the signed document will be kept on file.

(q) All LandWarNet users in the Army in Korea will take and pass Computer-User Test before being issued a network password and user identification.

(r) All LandWarNet users in the Army in Korea will maintain an AKO account and are highly encouraged to auto forward email from AKO to their korea.army.mil account when established.

(s) All LandWarNet users in the Army in Korea will maintain Common Access Card and will maximize the usage of PKI. Users are required to publish their certificates to Global Address List.

Paragraph 3-3.c.(2) Prohibited activities. Add subparagraphs (l) through (n) as follows:

(l) Use any application that is not specified in the accreditation for the network.

(m) Use of any un-authorized software (i.e. IRC, ICQ, P2P (any version), and Instant Messaging).

(n) Establish unauthorized wireless connections within the Army in Korea networks.

Paragraph 3-3.m.(1) Designated Approving Authorities (DAAs). Add subparagraphs (g) through (h) as follows:

(g) DAAs for individual enclave appoint an IAM and CA within their AOR.

(h) DAA for LandWarNet (class) will serve as the final approval authority for Protected Distribution Systems (PDS) that will be connected to the LandWarNet (class).

Paragraph 4-2.b MDEP MX5T funds. Add the following at the end of the paragraph (1):

Eighth Army CIO/G6, through RCIO-K, will provide annual Army of Korea funding guidance for MDEP MS4X. Request for COMSEC equipment must be coordinated with Eighth Army CIO/G6, and an authorization document must be on hand before submitting a requirement through the ISSP program.

Paragraph 4-3 Information Assurance training. Add the following at the end of the main paragraph:

All IA personnel must maintain an account in the Army Asset and Vulnerability Tracking Resource (A&VTR), and provide their Role, Type, and Training records. Appendix D provides IA training and certification requirements for the Army in Korea.

Paragraph 4-3.a Certification training requirements. Add the following:

Provide the complete training information to the A&VTR database.

Paragraph 4-5.b Access control. Add the following at the end of paragraph (7):

LandWarNet users in Korea must have JEDI loaded on their workstations, which can be pushed to the systems in Korea domain or downloaded from TNOSC web site.

Paragraph 4-5.d Remote access servers (RASs). Add the following:

Designated TSACS servers and VPN services will be used for remote access to the Army in Korea LandWarNet. No other remote connection is permitted.

Paragraph 4-5.r Acceptable Use Policy (AUP). Add the following at the end of paragraph (1):

AUP for the Army in Korea is available from the local DOIM or RCIO-K.

Paragraph 4-5.s Computer log-on banner. Add the following at the end of the paragraph:

LandWarNet users in Korea must have JEDI loaded on their workstations, which can be pushed to the systems in Korea domain or downloaded from TNOSC web site.

After paragraph 4-5, Minimum Information Assurance requirements. Add paragraph 4-5.1 as follows:

4-5.1. MINIMUM IA REQUIREMENTS FOR ARMY IN KOREA SYSTEMS

- a. Each enclave DAA will ensure all systems connecting to the Army in Korea LandWarNet are properly accredited according to DODI 5200.40 (DITSCAP) that security requirements are reviewed regularly and updated as required.
- b. For all Army in Korea systems, responsible DAAs will ensure that the Eighth Army-approved computer security baseline (or baseline developed by the system's PM), information assurance vulnerability alerts (IAVAs), and current antivirus software and definition files are loaded on all systems before they are connected to Army in Korea LandWarNet. Program-managed system configuration requirements are controlled by the systems PM. PM will ensure that program-managed systems use the security configurations specified by the systems PM must coordinate with RCIO/DOIM/TNOSC to integrate PM systems within the Active Directory forest for proper patch management and software update.
- c. As a minimum, all Army in Korea systems must have a managed service pack, patch, and antivirus program that automatically update systems with the most current, approved service pack, patches, and antivirus definition files. Unit IASOs and IAMs are responsible for making sure that all systems have the latest patches installed. Unpatched systems are taken off the network until patched.
- d. Non-Army in Korea systems connecting to an Army in Korea LandWarNet for exercises or on a temporary basis (not to exceed 60 days) must have as a minimum a current antivirus program, current Service Packs and patches applied, and be compliant with all current IAVM releases. All non-Army in Korea systems will be scanned for compliance before they are placed on an Army in Korea network.

Paragraph 4-6, Controls. Add subparagraph q as follows:

- q. Prohibited software in the Army in Korea includes the following:
 - (1) Any type of Peer-to-Peer (P2P) software (ie. Gnutella, eDongkey)
 - (2) Unauthorized streaming audio and video including telephonic software (ie. Skype)
 - (3) Games other than Army-sanctioned simulations and games preloaded.
 - (4) Hacker tools and malicious logic software.
 - (5) Unauthorized Freeware and Shareware.
 - (6) Unauthorized keystroke-monitoring tools.
 - (7) Unauthorized network-monitoring tools.
 - (8) Unauthorized file-sharing software (for example, digital video disks (DVDs), MP3 music, music CD-ROMs, and video software).
 - (9) Unlicensed commercial (pirated) software.
 - (10) Firewalls not managed by the SA.
 - (11) Any unauthorized webpage authoring/altering software (for example, Bearshare, Cydoor, Gator, Limewire, TopText).

Paragraph 4-16, Protection requirements. Add subparagraph h and i as follows:

- h. All removable computer-system media (for example, CD-ROMs, DVDs, floppy disks, tapes, universal serial bus (USB) drives (memory sticks, pen drives, thumb drives)) must be Government-owned and properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know. All removable media will be scanned for viruses before use on Government systems. In the Army in Korea, the use of personally owned media on the LandWarNet (Unclas) or LandWarNet (Class) is prohibited.

- i. Hard copies that require protection must be shredded as a way of disposal.

Paragraph 4-19, Cross-domain security interoperability. Add the following at the end of paragraph b:

All requests for cross-domain security solutions must be submitted through the RCIO Korea.

Paragraph 4-19, Cross-domain security interoperability. Add subparagraph g as follows:

g. Until an approved GIAP solution is received from the DISA SIPRNET Connection Approval Office and approval is obtained from the Joint Chiefs of Staff, cross-domain connections are not allowed in the Army in Korea. This includes cross-connecting networks (including hard-disk drives of differing classifications in simultaneous operation on the same computer) and associated peripheral devices.

Paragraph 4-20.g, Internet, Intranet, Extranet, and WWW security. Add subparagraph (17) as follows:

(17) The AKO Internet chat tool is the only chat tool authorized for use on the Army in Korea LandWarNet (Unclas).

Paragraph 4-20.i, Information Assurance tools. Add subparagraph (6) as follows:

(6) Requests to use IA tools not on the Army-approved list must be forwarded to the Army in Korea IAPM for submission to the Army CIO/G6. IA tools not on the Army-approved list will not be used until approved by the Army CIO/G6.

Paragraph 4-22, Reporting responsibilities. Add the following at the end of paragraph c:

Incidents and intrusions will be reported to the RCERT-Korea

Paragraph 4-24.c, Army implementation of IAVM. Add subparagraph (3) as follows:

(3) Army in Korea. The RCIO-K in coordination with each Area DOIM will ensure IAVA requirement be informed and implemented by the units in Army in Korea.

Paragraph 4-25, Compliance reporting. Add subparagraph f as follows:

f. Compliance data will be entered into A&VTR database and maintained by unit IA personnel. RCIO-K in coordination with Eighth Army CIO/G6 will oversee A&VTR reporting for the Army in Korea.

Paragraph 4-29, Wireless local area networks. Insert the following after “level of risk determination”:

The presence of wireless technology must be identified and described explicitly in the organization’s C&A documentation. Advice and assistance to Army in Korea customers are provided by unit IAMs and supporting IA specialists at Area DOIM and RCIO-K.

Paragraph 4-30, Employee-owned information systems. Add the following:

EOIs (including memory sticks, media, and PEDs) are prohibited on Army in Korea networks and will not be used to process classified or unclassified and/or sensitive information.

Paragraph 5-4, Accreditation. Add the following at the end of paragraph d:

In the Army in Korea, local accreditation will be developed by the responsible organization and submitted to DAA for approval.

(1) Completed accreditation packets will be coordinated with and sent directly to the unit’s supporting DOIM. CIO/G6 will perform Certification Authority for tactical and exercise networks, and accreditation package for tactical and exercise system/network will be reviewed by CIO/G6 before the packet goes to RCIO for approval. The unit IAM is the

unit's primary POC for accreditation issues. Advice and assistance to Army in Korea customers is available from the unit's supporting IA specialist at the DOIM or RCIO-K.

(2) Responsible unit IAM, DOIM IAM, and RCIO-K will keep copies and track the status of all accreditation packets in their AOR. The DOIM IAM will maintain accreditation information in the IA Remedy database.

(3) IA specialists at each Area DOIM and RCIO-K are available to provide commands and organizations IA advice and assistance concerning the development of their SSAA. If technical expertise is not available in the unit, the unit may ask the IA specialist to help with certification testing and developing the residual risk statement as required by the DITSCAP.

(4) When minor changes are made to the existing accreditation, Network Change Proposal (NCP) will be forwarded to responsible DOIM and RCIO-K for approval. Reaccreditation is required every 3 years or if any of the events in paragraph 5-5b occur.

Paragraph 5-7, Connection approval process. Add the following at the end of paragraph a:

Organization requiring access to the Army in Korea networks will prepare CAP package, and the DAA of LandWarNet in Korea will approve the connection request and issue an approval to connect.

Paragraph 6-3.e, Approval of protected distribution systems. Add subparagraph (13) under paragraph e as follows:

(13) PDS connecting to LandWarNet (Class) in Korea will be certified by designated Certifying Agent, and DAA will approve PDS as part of the organization's C&A process.

APPENDIX D

CONSOLIDATED INFORMATION ASSURANCE TRAINING AND CERTIFICATION REQUIREMENTS

Individuals filling the positions listed in table D-1 (with the exception of the computer user) must be appointed on written orders. Basic course requirements must be completed within 6 months after appointment for certification. IA Training BBP will be used as a source for Certification requirement.

Table D-1			
Information Assurance Training and Certification Requirements for the Army in Korea			
Echelon	Position	Training Requirements	References
Battalion or equivalent units; staff offices headed by a lieutenant colonel or equivalent	Information assurance security officer Position responsibilities are outlined in paragraph 3-2f.	Basic requirement for IT-I and IT-II: The Army Information Assurance Security Officer course or an equivalent course (for example, Information Assurance/Computer Network Defense (IA/CND) Levels I and II)	AR 25-2 and AK Supplement
Brigade or equivalent units. Each designated approving authority (DAA) will appoint an information assurance manager.	Information assurance manager Position responsibilities are outlined in paragraph 3-2d.	Basic requirement: The Army Information Assurance Manager course or CISSP module (10 domain) in the Army E-Learning web site (https://usarmy.skillport.com)	AR 25-2 and AK Supplement
Organization with designated approving authority	Designated Approving Authority	Basic requirement: DAA CBT (DISA CD ROM)	AR 25-2 and AK Supplement
Each DAA will appoint a certification agent for each information system (IS) (or group of ISs) and network.	Certification agent (also known as system certifier) The certification agent is an information assurance duty rather than an information assurance position title. Position responsibilities are outlined in paragraph 3-3n.	Basic Course Requirement: Same as for the information assurance manager	AR 25-2 and AK Supplement NSTISSI 4015
As determined by the unit or organization G6 or equivalent.	System administrator (SA) and network administrator (NA) Position responsibilities are outlined in paragraph 3-3a.	Basic requirement: In accordance with DOD 8570.1	AR 25-2 and AK Supplement
Regional and supporting signal battalion (1 st Signal Brigade). Information assurance network managers may be appointed to assist information assurance network managers.	Information assurance network manager and network officer Position responsibilities are outlined in paragraph 3-2e.	Basic requirement: Same as for the information assurance manager	AR 25-2 and AK Supplement
Individual	Computer user Position responsibilities and prohibited activities are outlined in paragraph 3-3c.	Basic requirement: Army in Korea Computer-User Test. Users must receive information-assurance refresher training and retake the test each year	AR 25-2 and AK Supplement AK Pamphlets 25-25