



Office, Chief Information Officer / G-6

DEPARTMENT OF THE ARMY  
OFFICE OF THE SECRETARY OF THE ARMY  
107 ARMY PENTAGON  
WASHINGTON DC 20310-0107

NOV 15 2012

SAIS-CBM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Communications Security (COMSEC) Workstations Information Assurance Training and Certification Requirements

1. References:

- a. Department of Defense (DoD) Instruction 8523.01, Communications Security, 22 April 2008.
- b. DoD 8570.01-M, Information Assurance Workforce Improvement Program, 9 December 2005 (Incorporating Change 3, 24 January 2012).
- c. Army Regulation (AR) 25-2, Information Assurance, 24 October 2007 (Rapid Action Revision (RAR) Issue Date: 23 March 2009).
- d. AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material, 9 July 2012.
- e. National Security Agency (NSA) Information Assurance Directorate (IAD), Local Management Device/Key Processor (LMD/KP) Operational Security Doctrine, DOC 119-10, 23 June 2010.
- f. NSA IAD, Process Security Doctrine for the Enrollment of Key Management Infrastructure (KMI) Managers, DOC-042-12, 8 June 2012.
- g. NSA IAD, Key Management Infrastructure (KMI) Capability Increment – Two (CI-2) Management Client (MGC) Node, DOC-032-12, 26 March 2012.
- h. Army Chief Information Officer/G6 Information Assurance (IA) Training and Certification Best Business Practice, Ver. 5.0, 30 March 2012, [https://www.milsuite.mil/wiki/Portal:Army\\_Information\\_Assurance](https://www.milsuite.mil/wiki/Portal:Army_Information_Assurance).

2. Purpose: This memorandum clarifies Information Assurance (IA) Training and Certification policy and prescribes the Army approach for complying with Department of Defense (DoD) and Army policy for personnel executing System Administrator (SA) and related IA functions on the Local Communications Security (COMSEC) Management

SAIS-CBM

SUBJECT: Communications Security (COMSEC) Workstations Information Assurance Training and Certification Requirements

Software (LCMS) Workstation (AN/GYK-49) and the Key Management Infrastructure (KMI) Management Client (MGC) (AN/GYK-72). Individuals performing SA and related IA functions must be properly trained and obtain a DoD-approved certification appropriate to their positions and consistent with their computing environment (refs. a.-d.).

3. Background: With maturation of DoD IA training policy and the upcoming KMI implementation, personnel performing IA functions on Army COMSEC Workstations must be trained and certified to meet Information Assurance Technical Level I (IAT-I) certification baseline requirements. (Note: "COMSEC Workstation" refers to the LCMS Workstation and the KMI MGC.)

a. Army COMSEC Account Managers (CAMs) use the LCMS Workstation, also known as the Electronic Key Management System (EKMS) Tier 2 and Local Management Device/Key Processor (LMD/KP), to perform COMSEC and key management operations. The LCMS Workstation design and policy were developed such that the CAM is responsible for performing these COMSEC and key management functions as well as SA functions on the workstation.

b. Additionally, the NSA LMD/KP Security Doctrine (ref. e) mandates the LCMS Workstation SA be trained formally on the LCMS, which is the primary user application. Because the LCMS Workstation SA and COMSEC Account Manager functions are integrated on the workstation, and access to LCMS training is limited, Army CAMs have been the only individuals performing the SA functions. Currently, CAMs are trained in COMSEC and SA roles by successfully passing the LCMS Workstation Operator Course and were not previously identified as requiring additional IA training and certification.

c. In FY12, the Army began selectively replacing LCMS Workstations with the KMI MGC at operational COMSEC accounts. The NSA Process Security Doctrine for the Enrollment of KMI Managers (ref. f) requires personnel performing the KMI Client Platform Administrator (CPA) and Client Platform Security Officer (CPSO) roles for the MGC to meet DoD IAT-I baseline training and certification, in addition to KMI specific training requirements. These roles perform SA-related functions on the MGC.

d. The IA training requirements and the integration of the KMI MGC have clarified that COMSEC Account Managers performing system administrator and related IA functions on the LCMS Workstation and KMI MGC are required to be IA trained and certified.

4. Execution: The Army has developed a two-pronged approach to meet these policy requirements. One prong addresses training implementation requirements for current CAMs (Primaries and/or Alternates) performing the SA role on the LCMS Workstation, and the other prong addresses training for personnel performing CPA and CPSO roles on the KMI MGC.

SAIS-CBM

SUBJECT: Communications Security (COMSEC) Workstations Information Assurance Training and Certification Requirements

a. LCMS Workstation CAMs (Primary and/or Alternates) currently performing the function of SA must meet the below prescribed IA requirements for the administration and security of the LCMS Workstation.

(1) The appointed SA must complete Information Assurance Technical (IAT) Level I certification baseline requirements (i.e., A+, Network+, or System Security Certified Practitioner (SSCP)). In addition to the IAT-I certification baseline requirements, an LCMS SA must obtain any certifications or specific training required to implement the IA security requirements for the LCMS Workstation operating system. The LCMS Workstation Computing Environment (CE), specific operating system's certification requirement is met by satisfactorily passing the TRADOC-approved (or DoD/Service-equivalent) LCMS Workstation Operator Course. Individuals must successfully complete the required LCMS Course PRIOR to accessing the LCMS Workstation (unless granted exception by ref. d above). Appointment orders must be maintained in accordance with (IAW) AR 25-2 for CAMs performing as SA. (Note: Individuals that obtain a higher level certification, such as IAT-II or -III, meet the IAT-I requirement without obtaining any of the lower level certifications).

(2) The appointed SAs must ensure they are enrolled in the continuing education program and maintain their baseline IAT-I certification in accordance with commercial vendor requirements and Army policy.

(3) The LCMS Workstation SA must be a U.S. citizen, employed by the U.S. Army with a minimum of final SECRET or interim TOP SECRET security clearance (dependent on the highest classification level of the COMSEC account). Contractors cannot serve as the SA for the LCMS Workstation.

(4) The LCMS Workstation SA must sign an Information Systems Privileged Access Agreement and Acknowledgement of Responsibilities which must include a statement acknowledging the individual's responsibility to maintain all required certification(s). A copy of this agreement will be maintained by the Information Assurance Manager (IAM) and the LCMS Workstation SA. This is a special item of interest and shall be reviewed during Command Inspections and COMSEC Audits.

(5) The LCMS Workstation SA must be registered in the Army Training and Certification System (ATCTS) database to track training and certification. Individuals must be enrolled in the database within 30 days of receipt of this memorandum or within 30 days of being appointed by the Commander.

(6) The LCMS Workstation SA will be required to perform all System Administrative functions for the operation and security of the LCMS Workstation.

(7) For personnel currently executing the SA function, training and certification must be completed within 6 months of the date of this memorandum. For newly appointed CAMs

SAIS-CBM

SUBJECT: Communications Security (COMSEC) Workstations Information Assurance Training and Certification Requirements

assuming the LCMS Workstation SA functions in the future, training and certification requirements must be met within 6 months of appointment. Failure to meet this requirement can result in the suspension of administrative rights and possible suspension of the COMSEC account.

b. Personnel performing the KMI MGC Client Platform Administrator (CPA) and Client Platform Security Officer (CPSO) roles must meet the below prescribed IA training and certification requirements for the administration and security of the KMI MGC. (Note: The Army began a limited transition of LCMS Workstations to the KMI MGC on 9 July 2012.)

(1) Commanders will identify and appoint a CPA and a CPSO for each KMI MGC. Appointment Orders must be maintained IAW AR 25-2 for individuals performing these roles. (Note: Personnel can perform CPA or CPSO roles on more than one MGC.)

(a) KMI MGC CAMs or other qualified individuals can serve as the CPA for the MGC if they meet the prescribed IA training and certification requirements.

(b) Individuals appointed as CPSOs cannot perform the CPA role, KMI Operating Account Manager (KOAM) role or any other role in the operation and security of the KMI Operating Account and MGC.

(2) Individuals appointed to perform the CPA or CPSO roles must complete IAT-I certification baseline requirements (i.e., A+, Network+ or SSCP. In addition to the IAT-I certification baseline requirements, the CPA and CPSO must obtain certifications or specific training required to implement the IA security requirements for their specific KMI MGC operating system. The KMI MGC CE specific operating system's certification requirements will be met by satisfactorily completing the KMI CPA or CPSO Computer Based Training (CBT) modules. Individuals must successfully complete the required KMI CPA or CPSO CBT modules PRIOR to accessing the KMI MGC. (Note: Individuals that obtain a higher level certification, such as IAT-II or -III, meet the IAT-I requirement without obtaining any of the lower level certifications.)

(3) The appointed CPA and CPSO must maintain their baseline KMI MGC IA certifications in accordance with commercial vendor requirements and ensure they are enrolled in the continuing education program for their particular certification.

(4) Personnel performing MGC CPA or CPSO roles must be U.S. citizens, employed by the U.S. Army with a final SECRET or interim TOP SECRET security clearance (dependent on highest classification level of the COMSEC account). KMI is a role based and ruled based system that allows technical separation of roles. Contractors can serve as CPA or CPSO for the KMI MGC only (not the LCMS Workstation).

SAIS-CBM

SUBJECT: Communications Security (COMSEC) Workstations Information Assurance Training and Certification Requirements

(5) If the CPA or CPSO does not have a TOP SECRET clearance, the CAM must sanitize the area to the SECRET level when the CPA or CPSO is performing administrative duties.

(6) The MGC CPA and CPSO must sign an Information Systems Privileged Access Agreement and Acknowledgement of Responsibilities which must include a statement acknowledging the individual's responsibility to maintain all required certification(s). A copy of this agreement will be maintained by the Information Assurance Manager (IAM) and the MGC CPA and CPSO.

(7) The CPA and CPSO must be registered in the Army Training and Certification System (ATCTS) Database to track training and certification. Individuals must be enrolled in the database within 30 days of being appointed to the role by the Commander.

(8) The CPA and CPSO will be required to perform all the System Administrative functions for the operation and security of the KMI MGC (including the Advanced Key Processor).

(9) The CPSO will be required to sign for and maintain a KMI MGC token in accordance with prescribed KMI MGC security doctrine (ref. g).

5. Funding: Funding for IA training and certification requirements will be IAW AR 25-2 and the CIO/G6 Cybersecurity Directorate, Information Assurance Training and Certification Best Business Practice at [https://www.milsuite.mil/wiki/Portal:Army\\_Information\\_Assurance](https://www.milsuite.mil/wiki/Portal:Army_Information_Assurance) (ref. h).

6. Waivers: Organizations that cannot meet the training and certification requirements mandated in the prescribed timeframe must submit a waiver request with justification endorsed by the first O6/GS-15 in the chain of command. Waiver requests will be forwarded to the CIO/G6 Cybersecurity Directorate Identity Management Division for evaluation and approval/disapproval.

7. Duration: This memorandum is effective immediately. This guidance will be incorporated into the next publication of AR 25-2, and this memorandum will be superseded upon its publication.

SAIS-CBM

SUBJECT: Communications Security (COMSEC) Workstations Information Assurance  
Training and Certification Requirements

8. The points of contact for this action are Jeanne Medeiros-Williams at  
Jeanne.P.Medeiros-Williams.civ@mail.mil, (703) 545-1730, and Tobias Grant at  
Tobias.O.Grant.ctr@mail.mil, 703-545-4600.



STUART M. DYER  
Major General, GS  
Director, Army CIO/G6 Cybersecurity

Directorate

**DISTRIBUTION:**

Principal Officials Headquarters, Department of the Army  
Commander

- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Pacific
- U.S. Army Africa
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
- Eighth U.S. Army
- U.S. Army Network Enterprise Technology Command/9<sup>th</sup> Signal Command Army
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, U.S. Military Academy

**CF:**

- Commander, U.S. Army Accessions Command
- Commander, U.S. Army Cyber Command
- Director, Office of Business Transformation
- Director, Army National Guard
- Executive Director, Army National Cemeteries Program