DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT GORDON
307 CHAMBERLAIN AVENUE
FORT GORDON, GEORGIA 30905-5730

REPLY TO
ATTENTION OF:

IMSE-GOR-IM

JUL 16 2008

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort Gordon Policy Memorandum No. 37– Information Assurance (IA) Training, Personnel Security Standards, Roles, and Responsibilities

1. References:

a. AR 380-67, Personnel Security Program, 9 Sep 88

b. AR 525-13, Antiterrorism, 4 Jan 02

c. DoDD 8500.1, Information Assurance, 24 Oct 02

d. DoDI 8500.2, Information Assurance Implementation, 6 Feb 03

e. DoDD 8570.01, Information Assurance Training, Certification and Workforce Management, 15 Aug 04

f. DoD 8570.01M, Information Assurance Workforce Improvement Program, 19 Dec 05

g. Information Assurance Best Business Practice (BBP), 07 Mar 07

h. AR 25-2, Information Assurance, 24 Oct 07

2. IAW the above references, all users and appointed IA personnel utilizing a government system and/or network are required to meet personnel security standards and complete training prior to gaining access to the system and/or network, and they must complete annual refresher training to maintain that access. In addition to being capable of demonstrating the required level of technical and managerial skills and experience, all IA personnel must verify their knowledge and skills through standard certification and testing in accordance with the Department of Defense policy (DoDD 8570.1). Those who fail to meet these requirements will have their access removed. This policy outlines the requirements as well as the roles and responsibilities assigned to each position.

a. Commanders/Directors/Managers. In addition to being general users, Commanders, Directors, and Managers may have additional training and roles and responsibilities assigned to them as outlined in AR 25-2. These individuals are responsible for the actions taken by users

within their respective units/organizations and for the compliance level met within them. IA also falls under the realm of Force Protection and must be complied with, as such.

b. Users. Users are the foundation of the Defense in Depth (DiD) strategy and their actions affect the most vulnerable portion of the Army Enterprise Infrastructure (AEI). Users will not be granted access until standards and IA training requirements are met. Users who fail to maintain those standards will have their access removed until such time they can meet both standards and IA training requirements. All users must successfully pass the DoD IA Awareness training and sign the Acceptable Use Policy (AUP).

c. Foreign Nationals. Foreign Nationals requiring network access must have a request submitted by the Unit Commander/Director/Manager to the Designated Approving Authority (DAA) through the office of the Installation IAM. Detailed instructions for submitting the request can be found in AR 25-2, paragraph, 4-15.

d. IA Personnel. IA personnel and IA managers who perform any of the responsibilities or functions described in DoD 8570.01.M chapters 3-5, are privileged users. These responsibilities include: developing, testing, deploying, operating, administering, troubleshooting, managing, and retiring DoD information systems. IA Personnel must be appointed on orders by their Unit Commander/Director, and must meet the minimum standards for the networks to which they are assigned or appointed. IA personnel will not be granted privileged access until all minimum standards have been met. Personnel who fail to maintain those standards will have their privileged access removed until such time that they can meet them. All IA personnel must sign the Privileged-Level Access Agreement AUP.

(1) Designated Approving Authority (DAA). The DAA is the approving authority for all operating information systems. The DAA is appointed by the DA CIO/G6. The DAA approves all network connectivity and assumes all risk for those devices attached to it. All requests to connect to the network must be approved by the DAA.

(2) Certifying Authority (CA). The CA is the technical authority responsible for vetting all risks and known vulnerabilities and recommending approval or disapproval to the DAA.

(3) Information Assurance Manager (IAM). The Installation IAM is assigned to the DOIM and is the installation's senior IAM. Full duties and responsibilities are outlined in AR 25-2; however, the IAM develops, maintains, implements, and enforces a formal IA security and training program, ensures all systems are compliant and certified and/or accredited, manages IA personnel, and approves software and hardware. The IAM must be trained and certified IAW the attached table.

(4) Information Assurance Network Manager and Officer (IANM/IANO). Though the IANMs and IANOs can be appointed at the unit level, this appointment primarily occurs at the Installation level. The IANM/IANO duties are outlined in AR 25-2. IANM/IANO supports the IAM and ensures compliance of all devices on the network. The IANM/IANO must be trained IAW the attached table.

(5) Information Assurance Security Officer (IASO). IASO duties and responsibilities are outlined in AR 25-2. Each unit is required to have a primary and alternate assigned for both the NIPRNET and SIPRNET, where applicable. IASOs report to and are managed by the Installation IAM in the performance of their IASO duties. The IASO must be trained and certified IAW the attached table.

(6) Systems Administrator (SA). SAs are the individuals appointed to maintain the computer devices and associated peripherals, and are responsible for the hands-on work required to keep them compliant and mission ready for the unit. SAs will report to their respective IASO, as well as the Installation IAM. They may fill the role of the IASO in their absence. Each unit is required to have both a primary and an alternate SA assigned for both the NIPRNET and SIPRNET, where applicable. SAs can have various privileged access depending upon their duties. The SA must be trained and certified IAW the attached table.

3. Loss and Reinstatement of Privileges. Users found in violation of DoD or Army regulations and/or Fort Gordon acceptable use policy will lose their network access for a minimum of two weeks. Network privileges will not be reinstated until the user is retrained by the Installation IASO, counseled by their unit Commander/Director, a reinstatement request is submitted to the Installation IAM from their Commander/Director, and the reinstatement request is approved by the Installation IAM. Any IA personnel found in violation will also lose their IA privileges as outlined in the Privileged-Level Access Agreement acceptable use policy. Those individuals who have their security clearance revoked or denied will also lose their network access as per AR 25-2.

4. The Point of Contact for this memorandum is Ms. Queen D. Harts, Installation Information Assurance Manager, at 791-0042 or email queen.harts@us.army.mil.

Encl
IA Training Table

JOHN S. HOLWICK
Colonel, SC
Commanding

DISTRIBUTION: A

Training Requirements for Designated IA Personnel

IAT Level I Organization SA	IAT Level II Network SA/NM/IANM	IAT Level III Enterprise SA/NM/IANM
A+ **Network +** **SSCP**	**GSEC** **SCNP** **SSCP** **Security+**	**CISA** **CISSP** **GSE** **SCNA**
IAM Level I IASO	IAM Level II Installation IAM	IAM Level III RCIO IAPM
GISF **GSLC** **Security +**	**CISM** **GSLC** **CISSP**	**CISM** **GSLC** **CISSP**

Glossary:
Certified Information Security Auditor (CISA)
Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CISSP)
Global Information Assurance Certification (GIAC) Information Security Fundamentals (GISF)
GIAC Security Expert (GSE)
GIAC Security Essentials Certification (GSEC)
GIAC Security Leadership Certificate (GSLC)
Security Certified Network Architect (SCNA)
Security Certified Network Professional (SCNP)
System Security Certified Practitioner (SSCP)