



Information Assurance Best Business Practice (IA BBP)

U.S. Army CIO/G-6
Cyber Directorate

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION Version 5.0 (update)

March 2012

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

1. Overview:

The IA workforce focuses on the operation and management of IA capabilities for Department of Defense (DoD) systems and networks. IA ensures that adequate security measures and established IA policies and procedures are applied to all Information Systems (IS) and networks. The IA workforce includes all privileged users, specialty positions, and IA managers who perform any of the functions described in DoD 8570.01-M, Change 2 Chapters 3 - 5 and 10-11 across all occupational specialties, or whether the duty is performed full-time or part-time as an additional/embedded duty (DoD 8570.01-M par C1.4.4.4). The IA training audience includes military, civilian, contractors and foreign nationals in Deployed and Generating Forces' organizations. Foreign nationals fall in two categories (contractor or civilian). A checklist to aid in determining if your duties are part of the IA workforce is included in this BBP (table 2). All new Department of Civilian hires appointed to IA positions must meet **qualification** requirements within 6 months. Contractor certification and training requirements shall be addressed in all contracts that include acquisition of IA services.

Existing contracts must be modified to specify **baseline** certification requirements. The DoD 8570.01-M, Change 3 paragraph C2.1.7 states: The IA workforce training and certification program establishes a baseline of validated (tested) knowledge that is relevant, recognized, and accepted across the Department of Defense. All IA workforce personnel requiring a certification voucher and appointed in Cyber Security (IA) positions shall be registered on the Army Training and Certification Tracking System at <https://atc.us.army.mil>. Personnel in Information Assurance Technical (IAT levels, Computer Network Defense-Service Provider (CND-SP) positions except for CND-SP Manager (CND-SPM) category are also required to obtain computing environment certifications or a certificate of training if working technical functions. The A+ certification can be used as a baseline and computing environment certification if the organization's manager accepts it as the required certification for their network/computing environment.

IA Workforce personnel in technical, specialty, and management positions must complete the required Continuing Professional Education credits annually and pay their annual dues as required by the certifying body to maintain certification status. Personnel who have been in the position over 1 year and have not attained qualification status shall be evaluated for reassignment in a non-IA position and noted in their performance evaluation.

Training and Certification requirements for the IA workforce, technical, specialty, and management levels described in DoD 8570.01-M, change 3 are listed in this BBP. **IA Workforce personnel who have completed the Information Assurance Fundamentals on the Signal Center website can earn 40 hours of Continuing Professional Education Credits for their CISSP and CompTIA certifications . The individual receives one CPE credit for each hour completed.**

The Army e-Learning program, comprised of commercial off-the-shelf computer-based and Web-based Distant Learning courseware, is the preferred method for all Army organizations to accomplish workforce training in information technology (IT), information assurance, foreign languages, and selected mandatory training requirements.

NoteCertification/certified denotes baseline and computing environment certifications throughout this document. Qualified denotes that the individual has the required documents (duty appointment letter, Privilege Access Agreement, met certification requirements and completed the On the Job training for their category and level.**

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

2. Changes to IA Policy:

a. The changes to the duties and responsibilities for the Information Assurance Support Officer were effective on 1 July 2011. Certification vouchers are no longer provided for personnel listed on appointment letters as IASO (Information Assurance Security Officer or Information Assurance Support Officer).

b. Soldiers in Military Occupational Specialty (MOS) 25B and 25U skill level one (SL1) shall operate and perform IA functions under the direct supervision of a certified IA professional. Soldiers in MOS 25B and 25U receive the required basic training through an eight week curriculum through their Advance Initial Training.

c. The Computing Environment certification can now be obtained through commercial certification testing or through training that map to the job functions required by the organization managers.

3. References:

a. DoD Directive 8570.01 (DoDD 8570.01) Information Assurance Training, Certification, and Workforce Management, 15 August 2004.

b. DoD 8570.01-M– Information Assurance Workforce Improvement Program, dated 19 December 2005, Change 3, 24 January 2012.

c. Memorandum: Manpower and Reserve Affairs, Payment of Expenses to Obtain Professional Credentials for Army Civilian Employees, 20 June 2003.

d. AR 25-2 – Information Assurance, 24 October 2007, Rapid Action Revision 23 March 2009.

e. AR 25-1 – Army Knowledge Management and Information Technology, 4 December 2008

f. Memorandum: Information Assurance (IA) Training and Certification Tracking System, 8 August 2007

g. DoD Acquisition Regulations System (DFARS) 48 CFR Parts 239 and 252 RIN 0750-AF52, Supplement; Information Assurance Contractor Training and Certification (DFARS Case 2006-D023

3. Point(s) of Contact (POC):

Cyber Directorate – Training and Certification

Phyllis Bailey
Group email address

Phyllis.e.Bailey2.civ@mail.mil, 703-545-1698
ciog-6.netcomiawip.inbox@mail.mil

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

4. Administrative Requirements:

a. IA training and certification requirements must be completed within 6 months of assignment to IA duties. Sustainment training is required as needed to keep the IA professional proficient in their job duties. All individuals performing technical functions must sign a Privileged Access Agreement (PAA) and Non-Disclosure Agreement (NDA). The PAA/NDA and duty appointment letter templates are located on the Army Training and Certification Tracking System under the document link. The duty appointment letter template is located at appendix E as well.

b. The Army e-Learning modules (Army e-Learning Program) for IA training are available via the AKO portal at <https://www.us.army.mil>. Contractors who require access to Army e-Learning for IA training will send their request through their Government Point of Contact (POC). They must also register on the Army Training Certification Tracking System (ATCTS), <https://atc.us.army.mil> and have their duty appointment letter and PAA/NDU (if applicable) uploaded into their profile. The Army e-Learning Program Contractor Info sheet is found at <https://atc.us.army.mil> under the document link and the Signal Center of Excellence, Ft Gordon website at <https://ia.signal.army.mil> under Courses. Completion of the Army e-Learning Program Test-preps alone will not be accepted as course completion - all modules must be taken. To generate end of module certificates, you must "Enroll" in each Learning Program course. There are various Learning Programs in the Baseline Certification folder in Army e-Learning. Enrollment procedures are found at <https://atc.us.army.mil> under the document link.

c. The IA workforce shall ensure that their profile data and IA training and certification information in the Army Training and Certification Tracking System (ATCTS) is current. New IA workforce personnel will register at <https://atc.us.army.mil> at the time of appointment. IA workforce personnel must release their certifications to the Defense Workforce Certification Web Application website (DWCA) at <https://www.dmdc.osd.mil/appj/dwc/index.jsp>. and document their certifications in the ATCTS.

d. Each Army organization shall program for funding the Annual Maintenance Fees during the Program Objective Memorandum (POM) cycle. Only the maintenance fee will be paid for the highest certification. The ISC (2) concentrations (if required for the appointed position) will be paid as well if funding is available.

e. IA workforce personnel (military and civilians) are encouraged to pursue educational opportunities through the IA Scholarship Program (IASP) to obtain advanced degrees with IA concentrations. Additional information about the IASP can be found on the ATCTS website under Web Links.

5. Description of tables:

- a. Table 1, How to Register in ATCTS
- b. Table 2: IA Workforce determination checklist
- c. Table 3: IA Workforce DOD Approved Certification List.
- d. Table 4: Qualified requirement table
- e. Table 5: IA Training and Certification Requirements matrix.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

Table 1: ATCTS Registration

1. How to register in ATCTS:

- a. Go to <https://atc.us.army.mil>.
- b. Go to Registration Information and click on [Register on this Web Site \(Click Here\)](#).
- c. Fill in all the fields then click "Register." Make sure you use a valid AKO email address and add your enterprise email as your alternate if you have one.
- d. The system will send an access code to your AKO email address.
- e. Once you receive your access code, log back into the system and answer the job function questionnaire. (The site is CAC only)
- f. Your Technical I-III or Management I-III or Specialty profile will be created along with a training plan. Do not skip this step; it allows you to see your minimum training requirements and baseline certification(s) required for your position function.

**INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0**

Table 2: IA Workforce Determination Checklist

Name		Email Address	
Company		Phone	
<i>Questions – Please respond to the questions below</i>			
QUESTION - Must answer YES to one or more questions to be part of the workforce.			YES/NO
1. Do you have an Privilege Access Agreement/NDU on file and in ATCTS			
2. Do you log on with a systems administrator account on a Government system? (Alternate Smart Card)			
3. Do you create user accounts or modify user permissions or roles for other users on a Government application, workstation, server, or network?			
4. Do you have the permissions and capability to install software on a Government server, workstation, or network device?			
5. Do you manage or otherwise have permissions to modify network devices for Government networks?			
6. Do you have the permissions and capability to install hardware on Government computer systems?			
7. Do you have the permissions and capability to install peripherals on Government computer systems?			
8. Do you have permissions to access and/or modify a database for a Government owned application on a Government computer system?			
9. Do you have the capability to delete or otherwise modify user accounts on Government systems?			
10. Are you responsible for maintenance, repair, or related upkeep of Government-owned computer or IT-related hardware at your site or installation?			
11. Can you perform system upgrades or modifications on Government computer systems?			
12. Can you perform network scans (e.g., STAT, RETINA) on Government computer systems?			
13. Can you perform surveillance or monitoring on Government computer systems?			
14. Do you move, install, or uninstall applications on Government computer systems?			
15. Do you create, initiate, or otherwise enact system, database, or application backup or restoration activities on Government owned application, workstation, server, or network?			
16. Are you an integral part of the design process or the development of IA Systems?			
17. Are you a Computer Network Defense Service Provider?			
18. Are you a member of the Red Team, Blue Team, or C& A Team?			
18. Do you approve, create and implement programs to ensure that systems, network, and data users are aware of, understand, and follow IA policies and procedures for your command			
19. Do create, approve and provide amplifying IA guidance that must be adhered to by your command and your subordinate commands			
20. Are you the Information Assurance Manager/Information Assurance Program Manager/ Chief Information Officer/DAA/ for your command			
21. Do you ensure that IA requirements are integrated into the Continuity of Operations Plan			
22. Do you assist in/prepare IA certification and accreditation documentation			
23. Do you allocate resources to achieve and maintain an acceptable level of security and to remedy security deficiencies?			

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

Table 3: DoD Approved Baseline Certifications

IAT Level I		IAT Level II		IAT Level III	
A+ Network+ SSCP		GSEC Security+ SCNP SSCP		CISA GCIH GSE SCNA CISSP (or Associate)	
IAM Level I		IAM Level II		IAM Level III	
CAP GISF GSLC Security+		CAP GSLC CISM CISSP (or Associate)		GSLC CISM CISSP (or Associate)	
IASAE I		IASAE II		IASAE III	
CISSP (or Associate)		CISSP (or Associate)		CISSP - ISSEP CISSP - ISSAP	
CND Analyst		CND Infrastructure Support		CND Incident Reporter	
GCIH CEH		SSCP CEH		GCIH CSIH CEH	
				CND Auditor	
				CISA GSNA CEH	
				CND-SP Manager	
				CISSP-ISSMP CISM	

* The Associate of (ISC)² is for those who do not meet the professional experience requirements for the CISSP. The Associate status is good for a maximum of six years from the date you are notified by (ISC)² that you have passed the examination. Within that timeframe, you will need to earn the required experience and submit the required endorsement form for certification as a CISSP.

***Computing Environment (CE) certification (vendor exam or certificate of training) required for IAT levels, CND levels and IASAE levels personnel who are working technical function.

**INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0**

Table 4: Qualified requirement Table (must complete all within 6 months of appointment to be fully qualified)

Category	Qualification 1	Qualification 2	Qualification 3	Qualification 4	Qualification 5	Qualification 6
IAT	Baseline Certification	Computing Environment Certification Or certificate	On-the-Job Training	Duty appointment Letter	Privilege Access Agreement	Complete training requirements in paragraph 10
IAM	Baseline Certification	Duty appointment letter	Complete training requirements in paragraph 8			
IASAE	Baseline Certification	Duty appointment letter	Complete training requirements in paragraph 12			
CND-SP	Baseline Certification	Computing Environment Certification Or certificate	On-the-Job Training	Duty appointment Letter	Privilege Access Agreement	Complete training requirements in paragraph 11

8. Management Levels: All must obtain a baseline certification

a. **Management Level I (IAM-I):** Complete qualification requirements within 6 months (see table 4) of IA appointment. Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team (MTT) IA course and/or vendor specific IA training hosted by the Army. Contractors cannot fill IAM-I positions at the Major Subordinate Command (MSC) and Installation levels, (25-2, paragraph 3-3f). See AR 25-2 for Information Technology level requirement.

Minimum Training Requirements:

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, 4-3(a)(5)(a).

(2). Army e-Learning Program – (CIO/G-6 Security+ (SY0-301) (10 modules) –

(3). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT >Baseline Certification Training>Certification and Accreditation – one module: ID# 206761_eng (Only if pursuing a CAP certification)

Certification Requirements:

The IAM-I personnel shall attain one of the Management Level I baseline certifications listed in Table 3. The type of baseline certification will be determined by the IA professional's supervisor during the performance evaluation process.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

b. **Management Level II (IAM-II).** Management Level II (IAM-II): Major Subordinate Commands (MSC)/Network Enterprise Center (NEC) Program Managed (PM) organizations/Information Assurance Manager (IAM)/ Agent of the Certification Authority (ACA) and other associated IA titles working IAMII functions. IAM II personnel shall not be designated at the Battalion or Company levels. Must complete qualification requirements within 6 months of IA appointment (see table 4). Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team IA course and/or vendor specific IA training hosted by the Army. The following courses are equivalent to the minimum training requirements for IA Managers in IAM-II and IAM-III positions: CNSS 4011 certificate course or the National Defense University, Information Resources Management College (IRMC) Advanced Management Program completion. See AR 25-2 for Information Technology level requirement.

Minimum Training Requirements:

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Certified Information Systems Security Professional (CISSP) modules– 10 modules – IAW AR 25-2, para 4-3a(1)(b).

(3). Army e-Learning Program- CIO/G-6 /Cyber Security IA/IT Training>Certified Information Security Manager (CISM) modules- 9 modules (if pursuing CISM certification).

(4). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training >Baseline Certification Training>Certification and Accreditation – one module: ID# 206761_eng (if pursuing a CAP certification)

Certification Requirements:

The IAM-II personnel shall attain one of the Management Level II baseline certifications listed in Table 3. The completion of certification testing is required.

c. **Management Level III (IAM-III): Operational Signal Theater Command/Functional Chief Information Office, Program Executive Office and AC/ASCC/DRU Information Assurance Program Manager (IAPM), Certification Authority (CA) and other associated IA titles performing IAM III functions:** Complete the qualification requirements within 6 months of IA Appointment (see table 4). Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team IA course and/or vendor specific IA training hosted by the Army. AR 25-2 for Information Technology level requirement.

Minimum Training Requirements:

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Certified Information Systems Security Professional (CISSP) modules – 10 modules. IAW AR 25-2, para 4-3a(1)(b).

(3). Army e-Learning Program- CIO/G-6 /Cyber Security IA/IT Training>Certified Information Security Manager (CISM) modules- 9 modules (if pursuing CISM voucher and certification).

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

Certification Requirements:

The IAM-III personnel shall attain one of the Management Level III baseline certifications listed in Table 3. The completion of certification testing is required.

9. Designated Accrediting Authority (DAA): DAAs performing other management functions such as IAM-II or IAM-III, must also meet the training and certification requirements for those categories and levels. Complete the minimum training upon DAA appointment by Army CIO/G6. The DAA must be a U.S. citizen and have a level of authority commensurate with accepting, in writing, the risk of operating IS under his/her purview.

(1). Complete the Army specific DAA training module. DAAs shall access this module through the Army's Virtual Training Website at <https://iatraining.us.army.mil>. This is only a training module and does not satisfy the DAA's certification requirement.

(2). DAA Certification: Complete the DoD DAA computer-based training (CBT) located on the Army's Virtual Training website at <https://iatraining.us.army.mil>. The completion will be imported into the DAA's ATCTS profile upon completion of the Army's 10 question test. The certificate of completion will be maintained as part of the DAA's official personnel file. The DoD DAA CBT is the DAA's certification and must be revalidated every 3 years.

10. Technical Levels: All must obtain a baseline and computing environment certification or certificate of training for the operating system(s) and/or security related tools/devices they support as required by their employing organization, DoD 8570.01-M, Change 3 para C3.2.4.8.3.

a. Technical Level I (IAT-I): System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO) **and other associated IA titles** working IAT-I functions. Complete the qualification requirements within 6 months of IA appointment 9 (see table 4). Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army MTT IA course and/or vendor specific IA training hosted by the Army. AR 25-2 for Information Technology level requirement.

Minimum Training Requirements:

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army E-Learning: Network+ 2009 CIO/G-6 /Cyber Security IA/IT Training>CompTIA Network+ 2009 (11 modules and Test-prep).

(3) Required For A+ Certification: Army e-Learning Program- CompTIA A+ modules

(a). 220-701, CIO/G-6 /Cyber Security IA/IT Training>Baseline Certification Training>NEW: A+ Certification-220-701 & 220-702 – 2009 Edition> CIO G-6 NETCOM IA 220-701-A+ Essentials 2009 (7 modules and Test-prep).

(b). 220-702, CIO/G-6 /Cyber Security IA/IT, >Baseline Certification Training>NEW: A+ Certification – 220-701 & 220-702 – 2009 Edition> CIO G-6 NETCOM IA 220-702- A+ Practical Application 2009 (5 modules and Test-prep).

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

(4). Completion of an On-the-Job Training (OJT) skills practical evaluation to meet functional requirements of DoD 8570.01-M. This requirement must be validated by the individual's supervisor or manager. An example of an OJT checklist can be found on the ATCTS website under Compliance Information.

Certification Requirements:

IAT-I personnel shall attain one of the Technical Level I baseline certifications listed in Table 3. The completion of commercial certification testing [or certificate of training is required per the guidance from the organization's management.](#) IAT-I personnel shall attain the appropriate computing environment certification or certificate of training as required by their employing organization (DoD 8570.01-M par C3.2.4.8.3). The A+ certification test consists of two tests and requires two certification vouchers. The Network+ certification test is one test.

b. **Technical Level II (IAT-II):** System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO) and other associated IA titles working IAT-II functions. Complete the [qualification](#) requirements within 6 months of IA appointment (see table 4). Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army MTT IA course and/or vendor specific IA training hosted by the Army. **IANM and IANOs manage groups of networks below the Army Command level. SA and NAs manage the Information Systems.** See AR 25-2 for Information Technology level requirement.

Minimum Training Requirements:

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training > ([CIO/G-6 SECURITY PLUS UH \(SY0-301\)](#)) (10 modules).

(3). Level II Schoolhouse, one week Security+ training course. Schedule and classroom sites located at <https://ia.signal.army.mil>. – Students must register through the Army Training Requirements and Resources Systems (ATRRS) – <https://www.atrrs.army.mil>. Request registration through your organization's training coordinator.

(4). Completion of an On-the-Job Training skills practical evaluation to meet functional requirements of DoD 8570.01-M, Change 3. paragraph C.3.2.3.2. This requirement must be validated by the individual's supervisor/manager.

Certification Requirements:

The IAT-II personnel shall attain one of the Technical Level II baseline certifications listed in Table 3. The completion of commercial certification testing or [certificate of training is required per the guidance from the organization's management.](#) The type of certification will be determined by the IA professional's supervisor during the performance evaluation process. Technical Level II personnel will also obtain the appropriate computing environment certification/s required by their employing organization (DoD 8570.01-M, Change 2 par C3.2.4.8.3).

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

c. **Technical Level III (IAT-III):** System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO) and other associated IA titles working IAT-III functions. Complete the qualification requirements within 6 months of IA appointment (see table 4). Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army MTT IA course and/or vendor specific IA training hosted by the Army. **IANM and IANOs manage groups of networks below the Army Command level. SAs and NAs manage the Information Systems.** All personnel in IAT-III positions must attain a commercial certification instead of a certificate of training. See AR 25-2 for Information Technology level requirement.

Minimum Training Requirements

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program – (CIO/G-6 /Cyber Security IA/IT Training)>Baseline Certification Training> Certified Information Systems Security Professional (CISSP) modules – 10 modules.

(3). Completion of an On-the-Job Training skills practical evaluation to meet functional requirements of DoD 8570.01-M, Change 3. paragraph C.3.2.3.2. This requirement must be validated by the individual's supervisor/manager.

Certification Requirements:

IAT-III personnel shall attain one of the Technical Level III certifications listed in Table 3. The completion of certification testing is required. Technical Level III personnel shall attain the appropriate computing environment certification required by their employing organization (DoD 8570.01-M change 3 par C3.2.4.8.3).

11. Computer Network Defense Service Providers Specialty: CND Service Providers typically work within the Network Operations Centers (NOC), Network Operations Security Centers (NOSC), Computer Security Incident Response Teams (CSIRTs), Computer Incident Response Teams (CIRTs), or Computer Emergency Response Teams (CERTs).

CND-SP specialty personnel shall attain:

- The appropriate baseline IA certification (technical or management).
- The appropriate CE certification or certificate of training as required by their employing organization.
- The appropriate specialty certification.
- Certifications are not cumulative. Higher certifications do not satisfy the certification for the specific CND-SP category.

a. **CND-SP Analyst (CND-A):** Complete the qualification requirements within 6 months of IA appointment (see table 4). The CND-A must be able to work on a specific number of CND systems but analyze events within the NE or enclave. Complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army MTT IA course and/or vendor specific IA training hosted by the Army (if applicable). The CND-A typically has mastery of IAT Level I

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

and IAT Level II, CE and/or NE with applicable certification, works under supervision, and typically reports to a Computer Network Defense-Service Provider Manager (CND-SPM).

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Baseline Certification Training>, GIAC Technical Modules. (16 modules).

(3). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training>Baseline Certification Training>CIO/G6 NETCOM Ethical Hacker (11 modules). This can be completed in lieu of the GIAC Technical Modules if pursuing a CEH certification.

(4). Complete an On-the-Job Training skills practical evaluation to meet functional requirements of DoD 8570.01-M, Change 3. paragraph C.3.2.3.2. This requirement must be validated by the individual's CND-SPM.

Certification Requirements:

The CND-A personnel shall attain one of the IAT-I or IAT-II and CND baseline certifications listed in Table 3. The IAT certification is dependent upon the environment the CND-A manages (CE, NE, and Enclave). The completion of commercial certification testing is required. CND-A personnel will also attain the appropriate computing environment certification or certificate of training.

b. CND-SP Infrastructure Support (CND-IS): Complete the qualification requirements within 6 months of IA appointment (see table 4). The CND-IS must have significant knowledge of particular networking technologies, operating systems, and CND tools, tactics, techniques, and procedures which are part of the systems they support. Their actions are usually authorized and controlled by policies and established procedures. They must complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army MTT IA course and/or vendor specific IA training hosted by the Army (if applicable). The CND-IS usually has mastery of IAT Level I and IAT Level II, CE and/or NE with applicable certification, works under supervision, and typically reports to a CND-SPM.

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Baseline Certification Training>, GIAC Technical Modules. (16 modules).

(3). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training>Baseline Certification Training>CIO/G6 NETCOM Ethical Hacker (11 modules). This can be completed in lieu of the GIAC Technical Modules if pursuing a CEH certification.

(4). Complete an On-the-Job Training skills practical evaluation to meet functional requirements of DoD 8570.01-M, Change 3. paragraph C.3.2.3.2. This requirement must be validated by the individual's CND-SPM.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

Certification Requirements:

CND-IS personnel shall attain one of the IAT-I or IAT-II and CND baseline certifications listed in Table 3. The IAT certification is dependent upon the environment the CND-IS manages (CE, NE, Enclave). The completion of certification testing is required. CND-IS personnel will also obtain the appropriate computing environment certification or certificate of training.

c. **CND-SP Incident Responder/Reporter (CND-IR):** Complete the qualification requirements within 6 months of IA appointment (see table 4). The CND-IR must have significant knowledge of particular CND tools, tactics, techniques, and procedures which support the tracking, management, analysis, and resolution of incidents. They must complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team IA course and/or vendor specific IA training hosted by the Army (if applicable). The CND-IR typically has mastery of IAT Level I, II, or III CE, NE and/or enclave with applicable certification, works under supervision, and typically reports to a CND-SPM.

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>GIAC Technical Modules. (16 modules).

(3). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>CIO/G6 NETCOM Ethical Hacker (11 modules). This can be completed in lieu of the GIAC Technical Modules if pursuing a CEH certification.

(4). Incident Handling (<https://iatraining.us.army.mil>)

(5). Complete an On-the-Job Training skills practical evaluation to meet functional requirements of DoD 8570.01-M, Change 3. paragraph C.3.2.3.2. This requirement must be validated by the individual's CND-SPM.

Certification Requirements:

CND-IR personnel shall attain one of the IAT-I, II, or III and CND baseline certifications listed in Table 3. The IAT certification is dependent upon the environment the CND-IR manages (CE, NE, Enclave). The completion of certification testing is required. CND-IR personnel will also attain the appropriate computing environment certification or certificate of training.

d. **CND-SP Auditor (CND-AU):** Complete the qualification requirements within six (6) months of IA appointment (see table 4). CND-AU personnel perform assessments of systems and networks within the NE or enclave and identify where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. They must complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team IA course and/or vendor specific IA training hosted by the Army (if applicable). The CND-AU typically has mastery of IAT Level I or IAT Level-II or IAT-III CE, NE and/or enclave with applicable certification, works under supervision, and typically reports to CND-SPM.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b).

(2). Army e-Learning Program: CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training> [GIAC Systems and Network Auditor \(GSNA\)](#) . (1 module). Course ID: FIN0232.

(3). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>CIO/G6 NETCOM Ethical Hacker (11 modules). **This can be completed in lieu of the GSNA modules if pursuing a CEH certification.**

(4). Complete an On-the-Job Training skills practical evaluation to meet functional requirements of DoD 8570.01-M, Change 3. paragraph C.3.2.3.2. This requirement must be validated by the individual CND-SPM.

Certification Requirements:

CND-AU personnel shall attain one of the IAT-I, IAT-II, or IAT-III level and CND baseline certifications listed in Table 3. The IAT certification level is dependent on the environment the CND-AU manages (CE, NE, Enclave). The completion of certification testing is required. CND-AU personnel will also attain the appropriate computing environment certification or certificate of training.

e. Computer Network Defense Service Provider Manager (CND-SPM) - complete the qualification requirements within 6 months of IA appointment (see table 4). The CND-SPM oversees the CND-SP operations within their organization. CND-SPMs are responsible for producing guidance for their NE or enclave, assisting with risk assessments and risk management for organizations within their NE or enclave, and are responsible for managing the technical classifications within their organization. They supervise technicians within their organization. They must complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team IA course and/or vendor specific IA training hosted by the Army (if applicable). The CND-SPM usually has mastery of IAM Level I or IAM Level II CE and/or NE knowledge and skills with applicable certification and works under supervision and typically reports to a Computer Network Defense senior manager or USSTRATCOM.

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>) IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>Certified Information Systems Security Professional (CISSP) modules – 10 modules.

(3). Army e-Learning Program- CIO/G-6 /Cyber Security IA/IT Training>Certified Information Security Manager (CISM) modules- 9 modules (if pursuing CISM certification).

Certification Requirements:

CND-SPM personnel shall attain one of the IA management and CND baseline certifications listed in Table 3. The IAM certification is dependent upon the environment the CND-SPM manages (CE, NE, Enclave). The completion of commercial certification testing is required.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

12. Information Assurance System Architect and Engineer (IASAE) Specialty

This Specialty comprises IASAE Levels I, II, and III. Complete the qualification requirements within six (6) months of IA Appointment (see table 4). All new hires must be certified within 6 months of appointment. Persons responsible for performing any of these functions, regardless of the occupational title (Engineer, Scientist, Computer Specialist, manager, pilot, infantry officer, etc.) shall be identified as part of the IA workforce. Personnel required to perform any IASAE specialty IA function(s) at any level must be certified to the highest level of function(s) performed. IASAEs that also perform IAT functions must also attain the appropriate computing environment certification and complete the IAT level requirements prior to being granted unsupervised privileged access. They must complete all Army e-Learning Program minimum training requirements prior to enrollment in an Army IT/IA schoolhouse, Army Mobile Training Team IA course and/or vendor specific IA training hosted by the Army (if applicable). Local Nationals or Foreign Nationals may be conditionally assigned to IASAE Level II but may not be assigned to IASAE Level III positions.

a. **IASAE Level I** personnel are responsible for the design, development, implementation, and/or integration of an IA architecture, system, or system component for use within their CE. Incumbents ensure that IA related IS will be functional and secure within the CE.

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>)
IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program – CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>Certified Information Systems Security CISSP modules – 10 modules.

Certification Requirements

IASAE Level I personnel shall attain one of the baseline certifications listed in Table 3 for their level. If performing technical (IAT) functions they are required to attain a technical level certification listed in Table 3 and Computing Environment certification or certificate of training. The IAT level baseline certification is dependent upon the environment the IASAE-I manage (CE, NE, and Enclave).

b. **IASAE Level II** personnel are responsible for the design, development, implementation, and/or integration of an IA architecture, system, or system component for use within the NE. Incumbents ensure that IA related IS will be functional and secure within the NE. Complete the **qualification** requirements within six (6) months of IA Appointment (see table 4).

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>)
IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>> Certified Information Systems Security CISSP modules – 10 modules.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

Certification Requirements

IASAE Level II personnel will obtain one of the certifications listed in Table 3 for their level. If performing technical (IAT) functions they shall obtain a technical level baseline certification listed in Table 3 and Computing Environment certification or certificate of training. The IAT level certification is dependent upon the environment the IASAE II manages (CE, NE, Enclave).

c. **IASAE Level III** personnel are responsible for the design, development, implementation, and/or integration of an IA architecture, system, or system component for use within CE, NE, and enclave environments. They ensure the architecture and design of Information Systems is functional and secure. This may include designs for program of record systems and special purpose environments with platform IT interconnectivity.

IASAE Level III personnel may also be responsible for system or network designs that encompass multiple CE and/or NE to include those with differing data protection/classification requirements. Complete the **qualification** requirements within six (6) months of IA Appointment (see table 4).

(1). Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>)
IAW AR 25-2, para 4-3a(1)(b)

(2). Army e-Learning Program - CIO/G-6 /Cyber Security IA/IT Training>Baseline Certificaton Training>> Certified Information Systems Security CISSP modules – 10 modules

Certification Requirements:

IASAE Level III shall obtain one of the baseline certifications listed in Table 3 for their level. If they perform technical (IAT) functions they will also be required to obtain a technical level certification listed in Table 3 and Computing Environment certification or certificate of training. The IAT level baseline certification is dependent upon the environment the IASAE-III manages (CE, NE, Enclave). The type of certification will be determined by the IA professional's supervisor during the performance evaluation process.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

Table 5: Training and Certification Matrix

	IA Mgmt I-III	IA Tech I-III	CNDSP: CND-A, CND-IS, CND-IR, CND-AU and CND-SPM	IASAE I-III
Training Requirement 1	IA Fundamentals online course (ALL)	IA Fundamentals online course (ALL)	IA Fundamentals online course (ALL)	IA Fundamentals online course (ALL)
Training Requirement 2	IAMI: Security Plus (Army e-Learning Program) OR Certification and Accreditation Army e-Learning modules (if pursuing CAP) IAMII-III: CISSP (Army e-Learning Program) OR Certification and Accreditation Army e-Learning modules (if pursuing CAP) or Certified Information Security Manager modules ; IAMII - CISSP (Army e-Learning Program) OR Certification and Accreditation Army e-Learning modules (if pursuing CAP) or Certified Information Security Manager modules ;	IAT I: CompTIA Network+ 2009 for the Network+ cert OR CompTIA A+ 220 701 and 702 for A+ cert (Army e-Learning Program) IAT II: Security Plus (Army e-Learning Program) and Security+ Level II Schoolhouse Course IAT III: CISSP (Army e-Learning Program)	CND-A, CND-IS, CND-IR, CND-AU: GIAC Technical Modules or GIAC Systems and Network Auditor (Army e-Learning Program) CND-SPM: CISSP (Army e-Learning Program) or Certified Information Security Manager modules All CND-SP categories except CND-SP Managers: CIO/G6 NETCOM Ethical Hacker if pursuing the Certified Ethical Hacker certification	CISSP (Army e-Learning Program) (ALL)
Certification (from approved list)	Yes (IA Certification within 6 months) **Certification requirements must be included in contracts**	Yes (IA Certification within 6 months) **Certification requirements must be included in contracts**	Yes (IA Certification within 6 months) **Certification requirements must be included in contracts**	Yes (IA Certification within 6 months) **Certification requirements must be included in contracts**
CE Certification or certificate of training for the operating system(s) and/or security related tools/devices	NO	Yes (within 6 months of appointment of IA position)	Yes (except CND-SPM) (within 6 months of appointment of IA position)	NO
Maintain Certification Status	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)
Continuous Education or Sustainment Training	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)
Privileged Access Agreement Required	NO	Yes	Yes	NO
Experience	IAM I: Usually an entry level management position with 2 to 5 or more years of management experience	IAT I: Normally has 0 to 5 or more years of experience in IA technology or a related field	Recommended years of experience in CND technology or a related field: CND-A: at least 2 CND-IR: at least 5 CND-AU: at least 2	IASAE I: Usually an entry level IASAE position with 0 or more years of IASAE experience.
Experience	IAMII: Usually has at least 5 years of management experience	IAT II: Normally has at least 3 years in IA technology or a related area	CND-IS: Recommended at least 4 years of experience supporting CND and/or network systems and technology	IASAE II: Usually has at least 5 years of IASAE experience.
Experience	IAM III: Usually has at least 10 years of management experience	IAT III: Normally has at least 7 years experience in IA technology or a related area.	CND-SPM: Recommended at least 4 years of experience in CND management or a related field	IASAE III: Usually has at least 10 years of IASAE experience

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

****Note: Denotes requirements for contractor personnel**

13. Supporting information assurance roles:

a. **Information Assurance Support Officer (IASO):** The role of the IASO is to provide Information Assurance oversight, guidance and support to the general user in accordance with the requirements for the Command's Information Assurance Program. The functions are listed in the memorandum: Changes to the Title, Responsibilities and Certification Requirements for Information Assurance Security Officers signed by the Army CIO/G6 dated June 7, 2011.

Training Requirement: Information Assurance Fundamentals (IAF) Course Online (<https://ia.signal.army.mil/courses.asp>).

b. **The Information Management Officer (IMO).** IMO functions are covered under AR 25-1 and DA Pam 25-1-1. If an individual works as an IMO and performs IA functions, the appointment letter, appendix D, will be annotated as such (e.g. IMO/SA, etc). The duty title will designate the type of training needed.

c. **Power User** Personnel with this title shall have limited administrative privileges to only their computer. There is no certification requirement with this title. The Information Assurance Fundamental course located on the Signal Center website shall be completed along with their annual IA Awareness training. Personnel do not need to have an appointment letter for this position. Power Users are not counted as part of the IA workforce. Power Users have rights to perform limited functions (i.e.: turn on wireless, connect to network printers). This position is selectable in ATCTS.

14. **IA Awareness Training:** Initial and annual IA awareness training for users is mandatory. The trained and aware employee is the first and most vital line of defense in protecting Information and Information Systems. This training shall be documented by the organization. The DoD IA Awareness Computer Based Training at <https://ia.signal.army.mil> shall be completed by all users with network access. Users shall complete the training module and the 10 question Army test to receive full credit.

15. **Proficiency training:** To sustain proficiency and meet vendor required continuing professional education (CPE) requirements. IA workforce personnel can enroll in courses at various locations online and vendor provided. One place for this training is the recorded instructor-led training through the DoD Virtual Training Environment (VTE) which provides on-line labs. These course completions are tracked in ATCTS and can count as continuing education points towards some or most of the commercial baseline certifications. Courses on the Army Virtual Training website (<https://iatraining.us.army.mil>) are a good source for proficiency training. Users shall register with their AKO email address in order for course completions to transfer into their ATCTS account. **User shall obtain at least 20-30 sustainment hours annually through on-line or classroom courses.**

a. Proficiency training includes (but is not limited to):

- (1) 1- week Network Manager Course at Fort Gordon
- (2) 14-day CND advance course
- (3) DoD VTE training at HU <https://www.vte.cert.org>.
- (4) Army e-Learning courses at <https://usarmy.skillport.com>. This site can be access through AKO as well.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

c. VTE training courses mapping to baseline certification is noted below: This is an on-line training platform that provides instructor-led classroom training and labs. VTE it is not a substitute for the Army e-Learning Program requirements for the Army Minimum Required Training.

- (1). (ISC)2 TM CISSP ® Prep Version 2 (IAM-II, IAM-III, CND-SP Manager, All IASE)
- (2). CompTIA Network+ Prep (IAT-I)
- (3). CompTIA Security+ Prep (SY0-301 (IAM-I and IAT-II)
- (4). IAT Level I Additional Resources (IAT-I)
- (5). IATII Additional Resources (IAT-I/IAT-II)
- (6). Fundamentals of Incident Handling
- (7). Hardening Windows Operating Systems
- (8) DISA HBSS Manager training

17. Qualifications:

a. Current: IA Technical and IA Managers with more than 6 months in an IA position shall be fully qualified. See table 4 for qualified requirements.

b. Newly appointed IA positions (civilians and military only) must become fully qualified within 6 months of being hired. .

c. Contractor personnel must be baseline certified upon hire in an IA/IT position. Contractors shall be appointed as well. Contractors shall attain a computing environment certification or certificate of training within 6 months of hire if working on an IA/IT contract. The government organization or government POC responsible for the Network environment will determine the type of training or computing environment certification requirement upon contract award.

18. Definitions:

a. Privileged access: Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access: (a) "Super user," "root," or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth; (b) Access to change control parameters (for example, routing tables, path priorities, addresses) of router, multiplexers, and other key information system or network equipment or software; (c) Ability and authority to control and change program files, and other users' access to data; (d) Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed; or (e) Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operation.

b. Limited privileged access: Privileged access with limited scope (for example, authority to change user access to data or system resources for a single information system or physically isolated network).

c. Computing Environment: Workstation or server host and its operating system, peripherals, and applications.

d. Network Environment (Computer): The constituent element of an enclave responsible for connecting CE by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

e. On-the-Job Training (OJT): Supervised hands on training based on specific performance criteria that must be demonstrated to a qualified supervisor. An example of an OJT checklist can be found on the ATCTS website under Compliance Information.

f. Enclave: Collection of CEs connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in OMB A-130 (reference (i)). Enclaves may be specific to an organization or a mission and the CE may be organized by physical proximity or by function, independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers

g. Depot Technician: Entry-level computer professionals, such as desktop support specialists and computer assemblers.

h. Remote Technician: Entry-level computer professionals, such as desktop support specialists, remote administrators, and customer support personnel.

i. IT Technician – Entry level computer professionals, such as desktop support specialists, remote administrators, and depot assemblers.

j. Qualified: A person meeting all requirements for their appointed IA category and level. Qualification consists of: 1). Duty appointment letter. 2). Privilege Access Agreement (if applicable). 3). Baseline certified. 4). Computing Environment certified or certificate of training (if applicable). 5). On the Job Evaluation (formerly known as on the job training).

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

**Army Voucher Program
Appendix A**

1. Objective: Military and Government Civilians to include, Non Appropriate Funds (NAF), Korean Augmentation to United States Army (KATUSA) and Government Foreign Nationals/Local Nationals performing IA functions described in DoD 8570.01-M, change 3 "Information Assurance Workforce Improvement Program" are eligible to receive a voucher through Army and/or their respective organization. Contractors and State employees are not eligible for vouchers through this process. IA Workforce personnel can receive a voucher for their current functional level and one level lower.

2. Voucher Request Procedures: Army will purchase a limited number of IA baseline certification vouchers to achieve some of the certifications outlined in, DoD 8570.01-M, Change 3 baseline certification chart. Some of the vouchers purchased by the Army are: CISSP, CISM, IASAE, CAP, Network+, A+ Security+ and CEH. All Army vouchers will be managed and distributed by Army CIO/G6, Cyber Directorate. Individuals receiving vouchers will schedule and test within 30 days of voucher issuance. . Individuals who do not pass on the first attempt can request one additional voucher for retesting after a 30-day retraining period. The Voucher request form and the pre-assessment test results must be in.pdf format, no larger than 2 MB and uploaded into the individual's profile by their ATCTS manager. Pre-assessment tests must be taken within 30 days of the voucher request and results must be uploaded in the individual's profile by their ATCTS manager prior to receiving an exam voucher.

3. Certification examination: Individuals should check with their local base or station education office for the schedule and location of certification exams in your area. Testing centers can also be found on the certifying body's website or testing center websites. Verify certification exam date and location before requesting a voucher.

Certificates will be mailed to you directly from the certification exam provider upon successfully passing your exam. Individuals are responsible for fulfilling all requirements once they have passed the certification exam. Once you have your certificate ensure that your records are updated with Human Resources and in ATCTS. Individuals must ensure all certification data (example: Candidate Career ID number) are entered.

4. Retraining alternatives: Training is provided to the IA workforce by distributed and/or blended learning solutions. Army e-Learning Program provides training in Security Plus, CISSP, A+, Network+, GCIA and other certifications. The Signal Center of Excellence, Ft Gordon School of Information Technology and all of the mirror sites provide training in Security + Network+, CISSP and A+. The Professional Education Center, Camp Robinson, AR provides training in Certified Ethical Hacker as well. Training is free to Military, Government civilians and contractors however organizations must pay individual's TDY cost.

5. Prioritization: Vouchers will be distributed within 1-3 days to individuals who are ready to test within 30 days of receiving the voucher and have completed all minimum training requirements and pre-assessment tests. **The appropriate Army e-Learning Program modules must be completed before a voucher is provided. Organizations should prioritize voucher requests and the certification of their IA workforce.**

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

6. Pre-assessment tests: Pre-assessment tests are available from the certification vendors. Information about Preassessment test is located on the ATCTS homepage under "Preassessment information". Individuals will complete the appropriate pre-assessment test prior to obtaining a certification exam voucher. A score of at least 75% or better is required to receive a voucher (for the first attempt). Pre-assessment tests are not available for some of the certifications such as CISSP.

7. Releasing Your Certification to DoD: If you are performing IA duties, and hold one of the DoD baseline certifications listed in DoD 8570.01-M, change 3, you must release your certification through the DWCA site at <https://www.dmdc.osd.mil/appj/dwc/index.jsp>. This is the official means of notifying DoD of your certification status. Authorizing the release of your certification status enables the Army CIO/G6, Cyber Directorate to import the validation of your certification from an authoritative source and continuing education enrollment date (comptia only) into your ATCTS profile. .

8. CompTIA Certifications: Certified personnel shall opt into the continuing education process starting 1 Jan 2011 in order to stay "current" in their certification and part of the DoD IA workforce. Personnel certified on 1 January 2011 and thereafter are automatically enrolled. Personnel with higher level certifications (see table 2) and received the certification prior to 1 January 2011 has the option of opting in. The higher certification shall be kept current. The continuing education process is the replacement for retesting every 3 years. DoD requires certification holders keep their certifications active and renewing those certifications if they expire. Military and DA civilians shall seek payment of their annual dues through their organization IA division. The IA divisions can use MS4X funds to assist their personnel with payment. Contractor personnel shall seek assistance through their contractor company.

9. Combatant Command (COCOM)

a. Combatant Command government civilians will register and request baseline certification vouchers through their service Executive Agent (EA) for the COCOM. Combatant Commands that use Army as the EA need to ensure government civilians positions filling designated (IAT/IAM/CND-SP/IASAE) are registered in DCPDS, DWCA system, ATCTS and request vouchers through ATCTS.

b. Military personnel, stationed at COCOMs will register and request vouchers through their Service system/process. COCOMs need to ensure military personnel filling positions designated (IAT/IAM/CND-SP/IASAE) are registered in the Electronic Joint Manpower and Personnel System (e-JMAPs) and Service personnel systems as appropriate.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION VERSION 5.0

Appendix B: Voucher Process and Procedures.

All IA workforce personnel requiring a certification voucher and appointed in Cybersecurity (IA) positions shall be registered on on the Army Training and Certification Tracking System at <https://atc.us.army.mil>.

1. How to obtain a certification voucher

- a. Register for ATCTS.
- b. Complete all Army minimum training requirements for your category/level. .
- c. Load duty appointment letter and privileged access agreement/NDU form if performing technical functions and have it validated by your ATCTS manager. Example is in Appendix D.
- d. Complete the appropriate pre-assessment test. The pre-assessment test date must be within 30 days of requesting a certification voucher.
- e. Fill out the voucher request form, send it through their manager/supervisor and then to their appointed IAM or IAPM, or commander for approval and signature. The ATCTS manager will upload the voucher request and pre-assessment test results in the individual's ATCTS profile under the voucher request/pretest area. Once the documents are loaded into the individual's profile, an email notification is automatically generated to the ciog-6.netcomiawip.inbox@mail.mil group email box. The A+ exam consists of two tests, however only one voucher request with preassessment test results need to be uploaded into the individual's ATCTS profile. The manager shall upload the first exam results in the individual's ATCTS profile in order for the individual to receive the second voucher.
- f. When the individual meets all the requirements the voucher will be added to their profile within 1-3 working days and a notification email sent to their AKO email address. The individual then needs to register for an exam at the appropriate testing center. All skillport training must be completed.

2. Retraining Requirements for 2nd Army Voucher.

- a. Army will fund one voucher for retest if you do not pass on the first attempt. The retraining period for obtaining a second voucher is 30 days (day one of retraining period starts day after the failed attempt). Complete the required re-training then follow voucher request procedures above. The pre-assessment test required results for a second voucher is 85%. If you registered on the VTE site with your AKO credentials then the VTE completion does not need to be loaded in ATCTS. The completion of the schoolhouse certification training will suffice for the VTE training as long as the date is after the first failed attempt.
- b. **Security+**: Complete the CompTIA Security+ Prep (SY0-301) recorded on-line, instructor led training on the VTE site at <https://vte.cert.org> and send results to your ATCTS manager to upload into your ATCTS profile with a new voucher request form and CompTIA pre-assessment test results.
- c. **Network+** : Complete the CompTIA Network+ 2009 recorded on-line instructor led training site at <https://vte.cert.org> and send results your ATCTS manager to upload into your ATCTS profile with a new voucher request form and CompTIA pre-assessment test results.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

d. **A+:** Complete the A+ recorded on-line instructor led training on the VTE website at <https://vte.cert.org> and send results to your ATCTS manager to upload into your profile with a new voucher request form and CompTIA pre-assessment test results

e. **CISSP:** Complete the ISC(2) TM CISSP (R) Prep version 2 on-line instructor led training on the VTE website at <https://vte.cert.org> and send results to your ATCTS manager to upload in your ATCTS profile.

f. **CAP:** Complete the CAP recorded on-line instructor led recorded training on the VTE website at <https://vte.cert.org> and send results to your ATCTS manager to upload into your ATCTS profile.

g. **CISM:** Complete the CISM recorded on-line instructor led recorded training on the VTE website at <https://vte.cert.org> and send results to your ATCTS manager to upload into your ATCTS profile.

3. Re-testing must occur within 30 days once the 2nd voucher is provided.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

**Change Request Procedures for DoD 8570.01-M Certifications
Appendix C**

As technology advances, the need to secure information systems and train the IA workforce to face security challenges is an evolving continuum. Therefore we must ensure that the IA workforce is achieving the appropriate level certification according to their position function. Organizations recommending additional certification/s to the DoD 8570.01-M baseline certification must perform a thorough analysis with the help of the certifying body of the recommended certification. The requirements are as follows:

- ◆ Select a certification that is accredited or going through accreditation under the American National Standards Institute (ANSI) International Organization for Standardization (ISO) 17024 accreditation program. The ISO 17024 program establishes a baseline set of standards that are in accordance with other major industry certifications.
- ◆ Map the functional requirements for the category listed in DoD 8570.01-M -- baseline certification chart to the recommended certification objectives.
- ◆ Document the history of use and acceptance outside of DoD (pass rate, test cost, delivery method, etc.)

A "Certification Proposal" template is located on the ATCTS homepage under information the document section to help the organization's map out the requirements before submitting the information to the Cyber directorate at ciog-6.netcomiawip.inbox@mail.mil.

The Army CIO/G6, Cyber Directorate POC will present the findings to the IA Workforce Improvement Program Advisory Council for inclusion into the manual. Once the committee provides their recommendation, DoD will provide the data to an independent third party (Institute of Defense Analysis) to conduct a formal mapping analysis to ensure the certification aligns with the functions in the 8570.01-M.

The final approval or disapproval takes from 6 months to one year. At this time, DoD is currently reviewing degree programs from the Center of Excellence colleges and universities for inclusion in the next change to DoD 8570.01-M.

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

Appendix D

Duty Appointment Template_ civilians (Can be used in the absence of organization appointment orders)

Use own letter head. Copy and paste information on organization letter head

MEMORANDUM FOR RECORD

SUBJECT: Designation of Information Assurance Personnel or Information Assurance Support Personnel (U).

1. References:
 - a. Army Regulation (AR) 25-2 Chapter 3
 - b. Department of Defense 8570.01-M Information Assurance, Workforce Improvement Program, Change 2, 20 April 2010.
2. Effective immediately, the below individual is appointed to perform IA duties/functions for < **Organization Name** >.
 - a. (U) Duty Position/Title:
 - b. (FOUO)

NAME:
GRADE
CIVILIAN JOB SPECIALTY CODE/MILITARY MOS:
PERSONNEL SECURITY STANDARDS (IAW AR 25-2, PARAGRAPH 4-14): **ITI/ITII/ITIII (Confirmed by JPAS)**
IA CATEGORY AND LEVEL (IAW DOD 8570.01-M): **IAMI/II/III or IATI/II/III or IASAE I/II/III or CND-SP position (Analyst/Infrastructure Support/Incident Responder/Auditor/SP Manager)**
3. Purpose: To perform IA functions/duties per AR 25-2 chapter 3 and DoD 8570.01-M.
4. Period: Until officially relieved or released from appointment, or upon transfer, termination, reassignment, retirement, or discharge.
5. Special Instructions:
 - a. Complete required IA training and certification for category/level per the Army's IA Training and Certification Best Business Practice.
 - b. Register in the Army Training and Certification Tracking System (HU<https://atc.us.army.mil>UH) and enter training and certification completions as outlined in the Army's IA Training and Certification Best Business Practice.
 - c. Upload duty appointment orders and privilege access agreement (if applicable).
 - d. <Additional Special instructions>
6. The point of contact is the undersigned.

Director/Commander/Manager Name and Signature
(Must be military or DAC- manual or digital signature)
Grade/ Civilian Series, Duty Position (Chief, Director, IAM, etc.)

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION
VERSION 5.0

Consolidated list of critical IA requirements to include in contracts:

The IA Program Manager and the IA Manager will work with the Contracting Officer's Representative when developing the Performance Work Statement to ensure the necessary items are incorporated when the documents are provided to the contracting officer.

Contracts for IA services will include at a minimum:

1. References to all pertinent guidance AR 25-2, and DOD 8570.01-M
2. Identification of the specific IA category and level for each IA function performed on the contract.
3. Identification of specific computing environment certifications/certificate of training required.
4. The requirement for contractors to register and create a profile in ATCTS to include uploading required documents.
5. A list of IA deliverables to include copies of IA certifications to be provided to the contracting officer and a personnel list from the vendor delivered to the contracting officer's representative (COR). The list should show the functions and IA category and level of each contractor.



Office, Chief Information Officer / G-6

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

SAIS-CB

APR 10 2012

MEMORANDUM FOR All Army Activities

SUBJECT: Implementation of Information Assurance Best Business Practice (IA BBP)

As the Director, Army CIO/G-6 Cyber Directorate and the Army FISMA Senior IA Officer (SIAO), the undersigned approves the identified IA BBP in support of Army Regulation 25-2 and the Army Information Assurance Program (AIAP). The BBP reflects the current standards to be implemented throughout the Army for all information systems and networks for the identified purpose.

**05-PR-M-0002: INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION,
Version 5.0**

A handwritten signature in black ink that reads "Steven W. Smith".

STEVEN W. SMITH
Major General, GS
Director, Army CIO/G-6 Cyber Directorate