Department of the Army
Pamphlet 25–2–6

Information Management: Army Cybersecurity

Cybersecurity Training and Certification Program

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–6
Cybersecurity Training and Certification Program

This new publication, dated 8 April 2019—

- Supports the guidance in AR 25–2 (throughout).
- Provides guidance and procedures for the training, certification, and management of the Department of the Army cybersecurity workforce conducting cybersecurity functions in assigned duty positions (throughout).

Headquarters
Department of the Army
Washington, DC
13 March 2019

Department of the Army Pamphlet 25–2–6

Information Management : Army Cybersecurity

Cybersecurity Training and Certification Program

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet provides guidance on the cybersecurity training and certification processes and procedures relating to military, Department of the Army Civilians, and contractors (to include foreign and local national personnel) performing cyberspace functions in accordance with the Department of Defense cyberspace workforce directives and manuals. This pamphlet aligns, manages, and standardizes cyberspace work roles, baseline qualifications, and training requirements.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Appendixes

Table List

Figure List

Glossary

Chapter 1
Introduction

1–1. Purpose
This pamphlet provides the procedures to carry out the Army Training and Certification Program guidance provided in AR 25–2 at the Department of the Army (DA) level. The processes and procedures in this pamphlet will help to develop a trained and qualified cybersecurity workforce.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See glossary.

1–4. Scope
This pamphlet applies to all DA organizational levels. It includes qualification guidance for the DOD cyberspace workforce framework (DCWF) work roles and categories as defined in DODD 8140.01, DOD 8570.01–M, DODI 8510.01, and AR 25–2.

1–5. Overview
a. The cybersecurity workforce focuses on the operation and management of cyberspace capabilities for DOD information systems (ISs) and networks. Cybersecurity ensures that adequate security measures and established cybersecurity policies and procedures are applied to all ISs and networks.

b. All organizations will develop, document, and disseminate cybersecurity awareness and training policy and procedures throughout their commands, to include their subordinate activities. The cybersecurity awareness and training policy must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Review the policy/procedures for cybersecurity awareness and training annually. The commander of the organization (or their designee) who has signing authority signs the policy.

c. The cybersecurity workforce includes all cyberspace information technology (IT) privileged users and specialty positions to include cybersecurity managers who perform any of the functions described in DOD 8570.01–M, regardless of occupational specialty, and regardless of whether the duty is performed full-time or part-time as an additional/embedded duty. The cybersecurity training and qualification program intends to provide cybersecurity personnel with a baseline understanding of the fundamental cybersecurity principles and practices related to the functions of their assigned position.

d. For planning purposes, the standard continuing education (CE) or sustainment training is normally a minimum of 20 to 40 hours annually, or 120 hours over 3 years.

e. The Army Credentialing Opportunities On-Line site has a complete list of qualifying credentials at https://www.cool.army.mil. Training and qualification requirements for the cybersecurity workforce are listed in this pamphlet.

f. Cybersecurity Fundamentals training, located on the Cybersecurity Training Center website (https://cs.signal.army.mil), must be completed every 3 years.

g. Cybersecurity workforce personnel who have completed the Cybersecurity Fundamentals course on the Cybersecurity Training Center website can earn 40 CE units/continuing professional education for their Information Systems Audit and Control Association (ISACA), International Information System Security Certification Consortium (ISC2) certification, Computing Technology Industry Association (CompTIA) Security+ CE, and CompTIA Advanced Security Practitioner (CASP) CE certifications. Individuals will receive one CE credit for each hour completed. The course may count as credit toward Global Information Assurance Certification (GIAC). Individuals should upload completion certificates to their vendor account for a decision.

h. All personnel holding information assurance technical (IAT) positions must obtain appropriate computing environment certifications or certificates of training for the operating system(s) and/or security-related tools/devices they support, as required by their employing organization. All technical personnel in the IAT Level III category will obtain a commercial computing environment certification (not just a certificate of training). Computer network defense service providers (CNDSPs) (except CNDSP managers) and information assurance system architect and engineers (IASAEs) who perform IAT functions must obtain appropriate computing environment certifications or certificates of training for the operating system(s) and/or security-related tools/devices they support.

Chapter 2
Accountability

2–1. Army Training and Certification Tracking System
All personnel with network access will register in the Army Training and Certification Tracking System (ATCTS) at https://atc.us.army.mil. If an organization has a valid reason for not using ATCTS for its authorized users then a memorandum of record signed by the authorizing official (AO) for that command must be sent to usarmy.belvoir.hqda-cio-g-6.mbx.training-and-certification@mail.mil.

2–2. Required documents
All personnel must upload the following documents to ATCTS after registration:

a. Acceptable use policy (AUP) if not signed on the Cybersecurity Center website at https://cs.signal.army.mil.

b. DA Form 7789 (Privileged Access Agreement (PAA) and Acknowledgment of Responsibilities) (if performing technical functions only).

c. Appointment letter (cybersecurity workforce only).

d. DD Form 2875 (System Authorization Access Request (SAAR)).

Chapter 3
Department of Defense Cyberspace Workforce Framework

3–1. Description
The DCWF derives from the National Initiative for Cybersecurity Careers and Studies–National Cybersecurity Workforce Framework. Both frameworks provide a blueprint to categorize, organize, and describe cybersecurity work according to specialty areas, tasks, and knowledge, skills, and abilities (KSAs). The frameworks organize cybersecurity into seven high-level categories, each comprised of several specialty areas. Each specialty area consists of multiple work roles. See https://niccs.us-cert.gov/ for additional information.

3–2. Roles
a. The DCWF associates work roles with categories/specialties, as shown in table 3–1. Cybersecurity personnel must determine the work role that fits their job functions.

b. KSAs and tasks related to each work role are listed in ATCTS under the KSA and Task tab in the work role box. Individuals must review the KSAs and tasks before choosing the work role(s), to ensure that the work role(s) chosen correlates with the job duties.

Table 3–1
Department of Defense cyberspace workforce framework categories and specialty areas

Category	Specialty Areas						
Securely Provision	Risk Management	Software Development	Architecture	Technology Research & Development	Systems Requirements Planning	Test and Evaluation	Systems Development
Operate & Maintain	Data Administration	Knowledge Management	Customer Service & Tech Support	Network Services	System Administration	Systems Security Analysis	
Oversee & Govern	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training	Cybersecurity Management	Acquisition & Program/Project Management	Executive Cyberspace Leadership	
Protect & Defend	Computer Network Defense	Incident Response	CND Infrastructure	Vulnerability Assessment &			

Table 3–1
Department of Defense cyberspace workforce framework categories and specialty areas—Continued

Category	Specialty Areas						
	(CND) Analysis		Support (CND–IS)	Manage-ment			
Analyze	Threat Analysis	Exploita-tion Analysis	All-Source Analysis	Targets			
Operate & Collect	Collection Operations	Cyber Operational Planning	Cyber Operations				
Investigate	Investiga-tion	Digital Forensics					

Chapter 4
Army e-Learning

4–1. Description

a. The Army e-Learning program, comprised of commercial off-the-shelf computer-based and web-based distance learning courseware, is the preferred method for all DA organizations to train their workforces in IT. Army e-Learning is the primary source of initial and sustainment IT training for Soldiers and DA Civilians before using alternative sources of instruction such as mobile training teams (MTTs) or courses contracted through the Chief Information Officer (CIO)/G–6. There is no cost to individuals or organizations to use Army e-Learning courses and products. Individuals must have an Army Knowledge Online (AKO) user identification (ID) (not AKO email) to register for Army e-Learning courses.

b. Army e-Learning modules for cybersecurity training are available via the AKO portal at https://www.us.army.mil or https://usarmy.skillport.com.

c. DA Civilians, military, and local/foreign national personnel can self-register in Army e-Learning and receive access to the entire Army e-Learning catalog.

4–2. Contract personnel

a. A government point of contact (POC) must request access for contractor personnel supporting Army cybersecurity contracts. Access is restricted to the cybersecurity CIO/G–6 folder that includes baseline and computing environment training. Contractors who require access to Army e-Learning for cybersecurity training will send their request through their government POC.

b. Contractors must also register in ATCTS at https://atc.us.army.mil and have their duty appointment letter and DA Form 7789, if applicable, uploaded into their profile. The Army e-Learning program Skillport—Contractor Access Request is located at https://atc.us.army.mil under Documents. The contractors' registration document is located on Cybersecurity Training Center website at https://cs.signal.army.mil under Courses.

4–3. Course completion

All lessons within an Army e-Learning course must be completed with at least 70 percent success. To generate end of module certificates, individuals must enroll in each learning program course. There are various learning programs in the CIO–G6, Cybersecurity IA/IT Baseline Certification folder in Army e-Learning. Find enrollment procedures at https://atc.us.army.mil under Documents.

Chapter 5
Training and Certification Program

5–1. What is cybersecurity training?

Cybersecurity training is the sum of the processes used to impart the body of knowledge associated with IT security to those who use, maintain, develop, or manage IT systems. A well-trained staff can often compensate for weak technical

and procedural safeguards. Cybersecurity training has been demonstrated to have the greatest return on investment of any technical or procedural IT security safeguard.

5–2. Program requirements

a. The cybersecurity certification program intends to produce cybersecurity personnel with a baseline understanding of the fundamental cybersecurity principles and practices related to the functions of their assigned positions. Each category, specialty, and skill level has specific training and certification requirements. Meeting these requirements requires a combination of formal training and experiential activities (such as on-the-job training and CE). Per DOD 8570.01–M, these training and certification requirements must be provided by the DOD and Army at no cost to government employees (military or DA Civilian). See DOD baseline certification charts at http://iase.disa.mil/iawip/pages/iabaseline.aspx.

b. Certification exam vouchers (provided for certification testing) and tokens (provided for annual maintenance fee payment) are provided to cybersecurity workforce personnel.

(1) Vouchers are provided to military and civilians, to include non-appropriated funds, Korean augmentation to United States Army, and government foreign nationals/local nationals appointed and performing cybersecurity functions to obtain/maintain the commercial certification exam that pertains to the certification corresponding to the highest level function(s) required by their position described in DOD 8570.01–M, Individuals appointed in multiple categories such as CNDSP and IAT or information assurance manager (IAM) can receive vouchers for each position if vouchers are available. For example, one voucher for CNDSP analyst and one for IAM I.

(2) A maximum of two vouchers for the appointed DOD 8570.01–M category and level will be provided. The two vouchers consist of one test and one re-test voucher. If a voucher was provided and the certification was obtained but then expired then that voucher will be counted as the first voucher. CIO/G–6 will provide one additional voucher to retest if vouchers are available.

(3) Tokens are provided annually to DA Civilians and military personnel (one per calendar year for one type of certification) for payment of annual maintenance fees, if available. Cybersecurity workforce personnel will be provided a token only for the highest certification for the assigned position. All other certification fees are the individual's responsibility. Request all tokens via the individual's ATCTS profile.

(a) Log into ATCTS.

(b) Click on the My Profile tab.

(c) Scroll down to AMF Token Requests.

(d) Only select one type of certification for payment.

c. Contractors and state employees are not eligible for vouchers or tokens through this process. A detailed process for requesting vouchers and tokens is found at https://atc.us.army.mil, under Documents.

d. Certification holders must adhere to all recertification policies set by their certification provider and ensure that their certifications stay active. The phrase "stay active" means the certification holder must ensure the annual fees for their certification are paid, and CE credits are obtained and uploaded into the appropriate certification provider's website.

e. The certification must be released through the DOD Workforce Certification (DWC) system in order to receive the token for payment. Expired certifications must be renewed (see DOD 8570.01–M).

Chapter 6
Authorized Users

6–1. Requirements

All authorized users must complete the approved DOD Cybersecurity Awareness training as a condition of network access prior to accessing DA information and ISs, and annually thereafter. Failure to complete annual Cybersecurity Awareness training will result in the user losing his or her computer access privileges until completed. Commanders may prescribe additional command-level training requirements to supplement the mandated standardized Cyber Awareness Challenge training.

6–2. Acceptable use policy

Each person who requires network access must sign (manually or digitally) an AUP at least annually. The AUP must be signed at the same time Cybersecurity Awareness training is completed (annually). Signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with organizational ISs to which access is authorized. Approved AUPs include the following:

a. The AUP on the Fort Gordon Cyber Security Training Center website (https://cs.signal.army.mil).

b. The AUP on the ATCTS homepage (https://atc.us.army.mil), under Documents.

c. The organization's internally developed AUP.

Chapter 7
Cybersecurity Training and Qualification Requirements

7–1. Cybersecurity workforce training and qualification assignment

a. All cybersecurity workforce personnel will register at https://atc.us.army.mil at the time of appointment. Registration is created via single-sign-on through the EAMS–A authentication system. Registration information instructions are found on the ATCTS page under Registration Information. In order to register the individual must have a valid AKO account. Contact the Army Enterprise Service Desk at 1–866–335–2769 and submit a ticket for the AKO login queue if you are having problems with creating or accessing your AKO account. ATCTS mangers have privileges to register individuals.

b. All DA Civilian and military cybersecurity workforce personnel appointed on letter must obtain qualification within 6 months of being assigned cybersecurity functions. If an individual has the required baseline certification when assigned to cybersecurity duties, the "Training Requirement 2" listed in appendix D is waived. All appointed DA Civilian and military cybersecurity workforce personnel not meeting the certification/qualification timeline will be reassigned to other duties consistent with applicable law.

c. Contractors performing cybersecurity functions will obtain the appropriate DOD-approved cybersecurity baseline certification prior to being engaged. Contractors have up to 6 months from appointment to the cybersecurity position to complete the Army minimum training requirements and the computing environment requirement that relates to their cybersecurity category and level/DCWF work role. The contract language must specify the DOD baseline certification requirements. The Defense Federal Acquisition Regulation Supplement 239.7103 specifies that the clause at 252.239–7001 must be used in solicitations and contracts involving performance of cybersecurity functions, as described in DOD 8570.01–M.

7–2. Privileged users

a. Privileged users with root, administrative, or super user access to systems will meet the requirements of an IAT, and will be trained and qualified as specified in DOD 8570.01–M. Each person with privileged access is required to acknowledge special responsibilities with DA Form 7789. This agreement must be signed by the person and the information systems security manager (ISSM)/information system security officer (ISSO) prior to privileged access being granted, and must be reviewed quarterly to ensure such access is commensurate with—

(1) Current mission requirements.

(2) The user's position/work role.

(3) A need for the user to perform functions that specifically require privileged/elevated access.

(4) Reassessment for least privilege and separation of duties.

b. All quarterly reviews will be conducted in ATCTS. The ATCTS manager will review each profile for denial or continuation of privileges by clicking the Quarterly Privileged Access Agreement Reviews link for their specific organization and making the proper notations.

c. See DA Pam 25–2–7 for additional information.

7–3. Authorizing officials

a. The AO must be a U.S. citizen and must have a level of authority commensurate with accepting the risk of operating ISs under his or her purview. See DA Pam 25–2–12 for grade structure and additional information.

b. Personnel seeking to become an AO will—

(1) Complete the AO training located at https://iatraining.us.army.mil. The individual will sign the Army certificate received at the end of the AO web-based training (WBT).Maintain the certificate of completion as part of the AO's official personnel file and upload the certificate in the individual's ATCTS profile.

(a) The training must be completed prior to AO appointment by CIO/G–6.

(b) The Army AO WBT meets the DOD AO certification requirement and must be revalidated every 3 years.

(2) The completion of the Enterprise Mission Assurance Support System (eMASS) training for AO and registration in the Army instances of eMASS (non-classified internet protocol router network and secret internet protocol router network) are required prior to commencement of any AO risk management framework activities. Training is available on the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) website at https://disa.deps.mil/ext/cop/mae/netops/emass/sitepages/home.aspx5. It is imperative that the AO print the DISA eMASS certificate at the end of the training session. If not printed, the AO may have to retake the training in order to receive the certificate. It is necessary to complete the training in one setting if the browser's cookies are not enabled.

7–4. Information system owners

a. Information system owners (ISOs) are responsible for developing, maintaining, and tracking the security plan for assigned IS and platform information technology (PIT) systems. ISOs will ensure review, testing, and assessment of assigned ISs and PIT systems are conducted at least annually, and register the IS or PIT system in eMASS (see DODI 8510.01). In coordination with the ISSO, the ISO is responsible for the development and maintenance of the security plan, and ensures that the system is deployed and operated in accordance with the agreed-upon security.

b. ISOs will—

(1) Be appointed in writing, along with identification of their responsibilities and the systems they are responsible for.

(2) Complete eMASS System Owner training within 15 days of appointment at https://iatraining.us.army.mil. The certificate, if received via the DISA IASE website, must be uploaded in the system owner's ATCTS by the organization's ATCTS manager.

c. Complete the Cybersecurity Fundamentals course on the Fort Gordon Cyber Security Training Center website (https://cs.signal.army.mil). See appendix D for further training information.

7–5. Information systems security manager

ISSM duties and functions are as follows:

a. Complete the training and certification requirements for IAM II or IAM III (see app D for additional information). The category and level depend on the functions performed, per DOD 8570.01–M.

b. Develop and maintain an organizational or system level cybersecurity program that includes cybersecurity architecture, requirements, objectives, policies, cybersecurity personnel, and cybersecurity processes and procedures, per AR 25–2.

c. Perform all ISSM duties and responsibilities in DODI 8500.01, DODI 8510.01, and AR 25–2.

7–6. Information system security officer

When circumstances warrant, a single individual may fulfill both the ISSM and the ISSO roles. ISSOs will—

a. Complete training and certification requirements (see appendix D for further information) for IAM I, IAM II, or IAM III, if also working as the ISSM for the organization. The category and level depend on the functions performed, per DOD 8570.01–M.

b. Assist the ISSMs in meeting their duties and responsibilities.

c. Perform all ISSO duties and responsibilities in DODI 8500.01, DODI 8510.01, and AR 25–2.

7–7. Communications security workstation management

Communications account managers (CAMs), key management infrastructure management client platform administrators (CPAs), and client platform security officers (CPSOs) who execute system administrator cybersecurity functions must be properly trained and qualified at the IAT I level (at a minimum) in accordance with DOD 8570.01–M. In addition to the baseline certification requirements, these individuals must obtain certifications or specific training for their specific operating system. The computer environment/specific operating system certification requirement will be met by satisfactorily completing the U.S. Army Training and Doctrine Command approved (or DOD/Serve-equivalent) local communications security (COMSEC) management Local Communication Management Operator Course and/or the CPA/CPSO computer-based training modules. These individuals (CAM/CPA/CPSO) must successfully complete the required COMSEC workstation operator course prior to accessing the workstation. All individuals must be appointed via letter to perform their duties.

7–8. Information management officer

Information management officer (IMO) functions are covered in AR 25–1 and DA Pam 25–1–1. If an individual works as an IMO and performs cybersecurity functions, the title on the appointment letter must identify the position held. The duty title/category/level will designate the type of training needed.

Chapter 8
Cybersecurity Workforce Certification Release to Department of Defense

8–1. Certification validation

a. Cybersecurity workforce personnel must release their certifications to the Defense Workforce Certification Application (DWCA) website at https://www.dmdc.osd.mil/milconnect/. Personnel will also upload their certificates into ATCTS if Defense Manpower Data Center (DMDC) validation is not present.

b. Certification validations are captured from the DWCA and imported into individual ATCTS accounts on the 1st and 15th of each month.

c. Individuals must re-release their certifications through DMDC each time the certification is renewed or if additional certifications are obtained on the DOD baseline certification chart.

d. ISACA will only renew certifications in DMDC for one year. Even though your certification shows a 3-year expiration date in your vendor account, it will only show annually in DMDC. Therefore, the release through DMDC must occur annually.

8–2. Release a certification

The following explains how to release a certification in DMDC:

a. Open a browser and navigate to https://www.dmdc.osd.mil/milconnect/.

b. Click on Sign In located in the top right corner of page to go to the milConnect Portal.

c. Click on the login for Common Access Card.

d. Click on the Correspondence/Documentation pull down and select DWC from the menu.

e. Click on Authorize Certifications.

f. Check the bottom of the page to see if your Certification/s is listed with the updated expiration date. If not, go to paragraph 8–2*h*.

g. Click on the vendor's name that your certification was issued from.

h. Certifications must be released each time a new expiration date is provided. If you have a valid annotation by your cert then you only have to click on the Re-Release Location under the Release button. If you have an unknown status then go to paragraph 8–2*i* but delete the unknown entry first.

i. Enter name exactly how it is on your certificate. For CompTIA certifications, if your full middle name is on your certificate then add your complete middle name in the middle name block or add with your first name in the first name block and leave the middle initial box blank. For all others (ISC2, ISACA, SANS, EC-Council) make sure the candidate ID number listed on your certificate matches what you have on your certificate.

j. Once all information is entered, check the box "I authorize the release of my certification information to the DOD" and click on "Send the above entry to vendor you selected."

Chapter 9
Retraining Requirements for Issuance of a Final (Second) Voucher

9–1. Retest

The Army will fund one voucher (if available) for a retest if an individual does not pass on the first attempt. The retraining period for obtaining a second voucher is 30 days. However, if the supervisor and command leadership feel that the individual is ready before the 30 days then the last voucher can be requested by completing the additional retraining and the voucher request. Follow the voucher request procedures for second vouchers at https://atc.us.army.mil under Documents. A total of two vouchers will be provided by CIO/G6. If CIO/G6 provided a voucher to take the exam and the individual passed but failed to keep the certification current then, if vouchers are available, another one can be provided for retesting. However, the first voucher for taking and passing the exam will be counted as one of the two vouchers.

9–2. Retraining

The following training counts as meeting the retraining requirement:

a. The Federal Virtual Training Environment (FedVTE) training for the requested certification exam voucher.

b. The current Army e-Learning program completion for the certification exam voucher if not completed for the first voucher.

c. A completion course through an Army MTT as long as the course was not taken for the first voucher. Upload the completion certificate to ATCTS.

Chapter 10
Qualifications

10–1. What does qualified mean?

Depending on the information assurance (IA) position, personnel qualifications include a combination of education and/or training, system/tool/device certification or certificate of training, baseline cybersecurity certification, on-the-job evaluation, experience, and background investigation requirements aligned to a specific position's job functions.

10–2. Requirements

Qualification requirements are shown in table 10–1. Personnel must complete all training requirements within 6 months of appointment to be fully qualified. Background investigation is required for all categories.

Table 10–1
Qualification requirements

Category	Qualification 1	Qualification 2	Qualification 3	Qualification 4	Qualification 5	Qualification 6
IAT	Duty appointment letter	Baseline Certification	DA Form 7789	On-the-job training (only for initial position (IAT I))	Computing Environment Certification or Certificate of Training (not for CNDSP managers)	Complete training in appendix D
IAM	Duty appointment letter	Baseline Certification				Complete training in appendix D
IASAE	Duty appointment letter	Baseline Certification				Complete training in appendix D
CNDSP	Duty appointment letter	Baseline Certification	DA Form 7789 (not for CNDSP managers)	On-the-job training (not required for CNDSP managers)	Computing Environment Certification or Certificate of Training (not for CNDSP managers)	Complete training in appendix D

Chapter 11
Combatant Commands That Use Army as Their Lead Agent

11–1. Civilians

Combatant command (COCOM) civilians will register and request baseline certification vouchers through their service lead agent for the COCOM. COCOMs that use Army as the lead agent must ensure civilian positions filling designated IAT/IAM/CNDSP/IASAE are registered in Defense Civilian Personnel Data System, DWC system, ATCTS, and request vouchers through ATCTS.

11–2. Military personnel

Military personnel stationed at COCOMs will register and request vouchers through their Service system/process. COCOMs must ensure military personnel filling positions and work roles designated in DOD 8570.01–M and DOD 8140.01 are registered in the Electronic Joint Manpower and Personnel System and Service personnel systems, as appropriate.

Chapter 12
Continuing Education Credits and Sustainment Training

12–1. Sources
To maintain proficiency, cybersecurity workforce personnel can enroll in the recorded instructor-led training through FedVTE, which provides online labs. These course completions are tracked in ATCTS. Courses on the Army virtual training website (https://iatraining.us.army.mil) are a good source for CE credits as well. Users will register with their enterprise email address in order for course completions to transfer into their ATCTS account.

12–2. Accepted courses and training
a. Training associated with a certification can be counted if the training is not the same version of the certification taken. For example, if you took a 2009 version of the Certified Information Systems Security Professional (CISSP) certification then you can take the CISSP 2015 training in FedVTE or Army e-Learning for CE credits.

b. Work experience for all certifications listed on the DOD baseline certification chart (http://iase.disa.mil/iawip/pages/iabaseline.aspx) counts for three CE credits per year for a total of nine points for the 3-year period.

c. The completion of the Cybersecurity Fundamentals course counts for as much as 40 CE credits for ISACA, ISC2, CompTIA, SANS, and EC-Council certifications.

Chapter 13
Mobile Training Teams

13–1. Overview
a. The CIO/G–6 Cybersecurity Directorate has contracted highly proficient MTTs to provide DOD 8570.01–M baseline certification training and computing environment training for Army organizations.

b. The MTTs are contracted to provide mobile training to Army organizations toward decreasing the cost of travel. MTTs are dedicated to training the cybersecurity workforce to a standard that is in line with the requirements of DOD 8570.01–M and AR 25–2.

13–2. Availability
The MTTs provide training to personnel working in cybersecurity positions who perform technical, managerial, and specialty functions in computing, network, and enclave environments.

13–3. Prohibitions
MTT training is not for individuals trying to obtain CE credits or for career progression. Online training provided through Army e-Learning (Skillport), FedVTE, and IASE (sponsored by DISA) are free and accessible to all military, DA Civilians, and DOD contractors working on a government cybersecurity service contract. Cybersecurity workforce personnel will use these venues to obtain the training to satisfy most, if not all, of their CE credits.

13–4. Hosting
All MTT courses must be hosted by an Army organization. Personnel from other services and DOD agencies (Air Force, Marines, Navy, and Coast Guard) who are part of their cybersecurity workforce may attend if seats are available. Training must be completed via the individual's respective service portal and provided to the Army POC to upload into their ATCTS profile. See the MTT procedures on the ATCTS homepage at https://atc.us.army.mil.

Appendix A

References

Section I

Required Publications

AR 25–1
Army Information Technology (Cited in para 7–8.)

AR 25–2
Army Cybersecurity (Cited in para 1–1.)

DA Pam 25–1–1
Army Information Technology Implementation Instructions (Cited in para 7–8.)

DA Pam 25–2–7
Army Information System Privileged Access Agreement (Cited in para 7–2*c*.)

DA Pam 25–2–12
Authorizing Official (Cited in para 7–3*a*.)

DOD 8570.01–M
Information Assurance workforce Improvement Program (Cited in para 1–4.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8140.01
Cyberspace Workforce Management (Cited in para 1–4.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8500.01
Cybersecurity (Cited in para 7–5*c*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Cited in para 1–4.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (http://armypubs.army.mil).

AR 25–30
Army Publishing Program

AR 380–40
Safeguarding and Controlling Communications Security Material

CJCSI 6510.01F
Information Assurance (IA) and Support to Computer Network Defense (CND) (Available at http://www.jcs.mil/library/cjcs-instructions/.)

CNSSI 1253
Security Categorization and Control Selection for National Security Systems (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

CNSSI 4009
Committee on National Security Systems (CNSS) Glossary (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

Defense Federal Acquisition Regulation Supplement 239.7103
Contract clauses (Available at http://www.acq.osd.mil/.)

NIST Special Publication 800–16
Information Technology Security Training Requirements: A Role- and Performance-Based Model (Available at https://www.nist.gov/publications.)

NIST Special Publication 800–37
Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Available at https://www.nist.gov/publications.)

NIST Special Publication 800–50
Building an Information Technology Security Awareness and Training Program (Available at https://www.nist.gov/publications.)

OMB Circular No. A–130 (Appendix III)
Security of Federal Automated Information Resources (Available at https://obamawhitehouse.archives.gov/omb/circulars_a130_a130appendix_iii.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (http://armypubs.army.mil). DD forms are available on the Office of the Secretary of Defense website (http://www.esd.whs.mil/directives/forms).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 7789
Privileged Access Agreement (PAA) and Acknowledgment of Responsibilities

DD Form 2875
System Authorization Access Request (SAAR)

Appendix B

Summary of Functional Requirements

B–1. Information

Table B–1 provides some of the functional requirements for each specialty category. It is not all inclusive.

B–2. References

Functional requirements are specified in DODI 8510.01 and DOD 8570.01–M.

Table B–1
Summary of functional requirements

Functional Title	Requirements
AO	Authorize connection/testing Accredit system Authorize IA controls Accept risk
IAM Levels I, II, III (ISSM, ISSO, and so on)	Oversee configuration testing Oversee system Revalidate IA controls Manage risks
IAT Levels I, II, III (system administrator, network administrator, and so on)	Manage connections/conduct testing Administer system Manage IA controls Operate (in) risk
IASAE Level I, II, III	Develop system Design IA controls Engineer (out) risk Conduct end-to-end analysis to identify mission-critical functions and components
CNDSP	Monitor system Assess IA controls Detect threat
ISO	Ensure compliance with information security requirements Develop and maintain the security plan Ensure the system is deployed and operated in accordance with the agreed-upon security controls Serve as the focal point for the IS Categorize systems in coordination with the program manager/system manager, information owner, mission owner(s), ISSM, and AO or their designated representative
Security Control Assessor	Responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IS to determine the overall effectiveness of the controls

Appendix C

Frequency of Training Completion and Certification Validations

C–1. The Army Training and Certification Tracking System

ATCTS communicates with various DOD and Army systems that collect training and certification completions. ATCTS pulls this information via web services or through a manual feed.

C–2. Inter-relation of systems

Figure C–1 illustrates how the systems inter-relate.

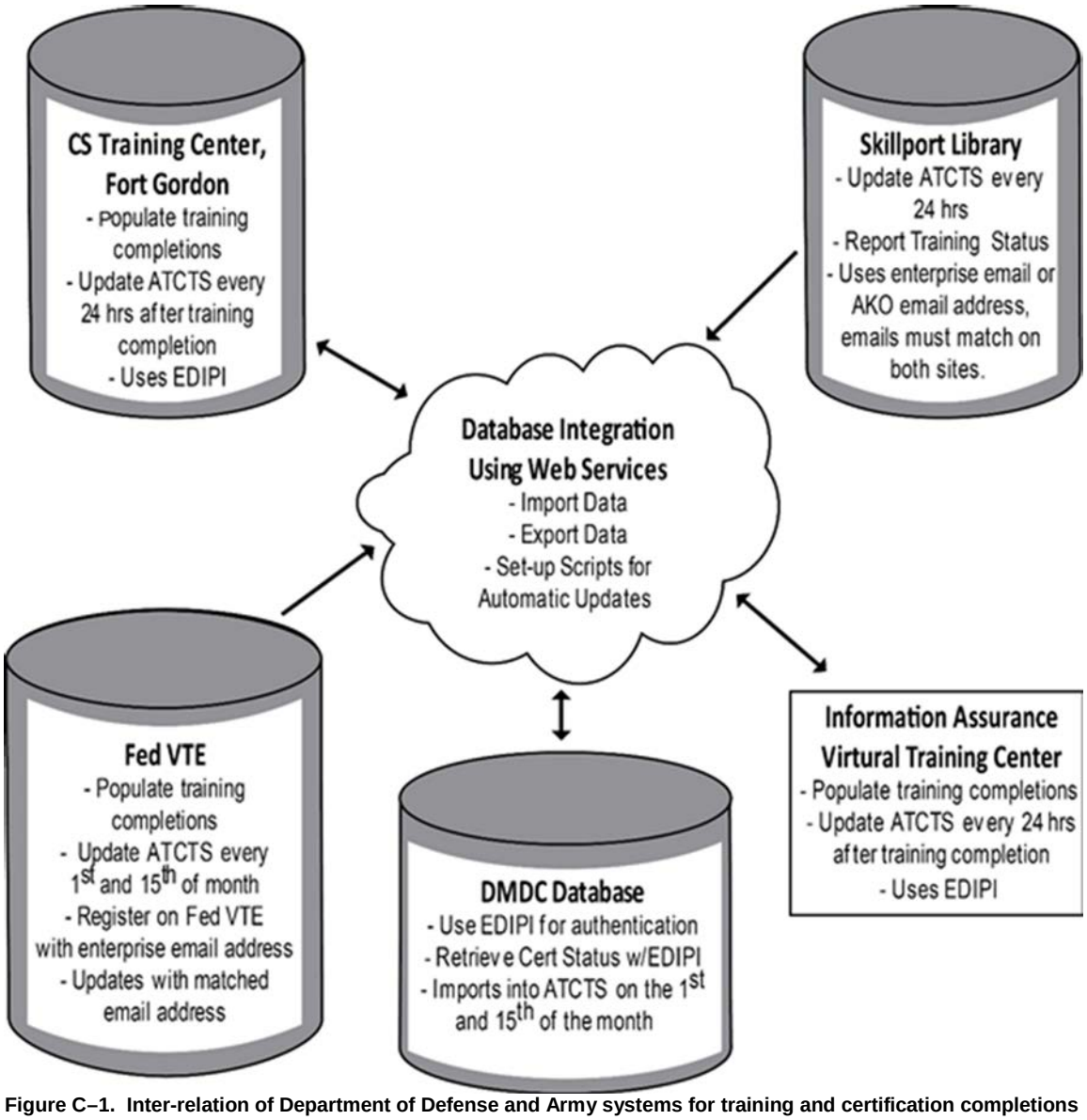

Figure C–1. Inter-relation of Department of Defense and Army systems for training and certification completions

Appendix D

Qualification Chart for DOD 8570.01–M Categories and Levels

D–1. General

IA workforce requirements and certifications are discussed throughout this pamphlet.

D–2. Training for qualification

Table D–1 depicts the requirements for a cybersecurity workforce person to be fully qualified to perform their duties in their assigned position. The most current training must be completed.

Table D–1
Qualification chart for cybersecurity workforce

	IAM I – III	**IAT I – III**	**CNDSP: CND Analyst (CND–A), CND–IS, CND Incident Responder (CND–IR), CND Auditor (CND–AU) and CNDSP Manager**	**IASAE I – III**
Training Requirement 1	Cybersecurity Fundamentals online course	Cybersecurity Fundamentals online course	Cybersecurity Fundamentals online course	Cybersecurity Fundamentals online course
Training Requirement 2	IAM I: Security Plus (Army e-Learning program) or FedVTE Certified Authorization Professional (CAP) training (if pursuing CAP) IAM II – III: CISSP (Army e-Learning program) IAM II only: FedVTE CAP training (if pursuing CAP) or Army e-learning CASP training (if pursuing CASP requirement) IAM II and IAM III only: Certified Information Security Manager (CISM) Army e-Learning program (if pursuing a CISM)	IAT I: current CompTIA Network+ (Army e-Learning program) for the Network+ certification or current CompTIA for A+ certification (Army e-Learning program) IAT II: current Security Plus (Army e-Learning program) IAT III: CISSP (Army e-Learning program) or Certified Information Systems Auditor (CISA) Army e-Learning program (if pursuing CISA) or Army e-Learning CASP training (if pursuing CASP)	CND–A, CND–IS, CND–IR, CND–AU: GIAC Technical Modules or GIAC Systems and Network Auditor (Army e-Learning program) CNDSP manager: CISSP (Army e-Learning program) or current CISM Army e-Learning program (if pursuing a CISM requirement)	CISSP (Army e-Learning program) Additional training to be completed but not required for Army minimum required training: Security Controls Assessor or Control Tester training in eMASS
Certification (from approved list)	Yes (cybersecurity certification within 6 months) Certification requirements must be included in contracts	Yes (cybersecurity certification within 6 months) Certification requirements must be included in contracts	Yes (cybersecurity certification within 6 months) Certification requirements must be included in contracts	Yes (cybersecurity certification within 6 months) Certification requirements must be included in contracts

Table D–1
Qualification chart for cybersecurity workforce—Continued

	IAM I – III	IAT I – III	CNDSP: CND Analyst (CND–A), CND–IS, CND Incident Responder (CND–IR), CND Auditor (CND–AU) and CNDSP Manager	IASAE I – III
CE Certification/ Certificate of Training for the Operating System(s) and/or Security-Related Tools/Devices	No	Yes (within 6 months of appointment of IA position). Personnel in IAT III positions must obtain a commercial certification	Yes (except CNDSP manager) (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)
CE 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 (except CNDSP manager)	No
Background Investigation	As required by cybersecurity level	As required by cybersecurity level	As required by cybersecurity level	As required by CNDSP level
Experience	IAM I: 0–5 years of management experience IAM II: at least 5 years of management experience IAM III: at least 10 years of management experience	IAT I: 0 to 5 years of experience in IA technology or a related field IAT II: at least 3 years of IA/IT experience IAT III: at least 7 years of IA/IT experience	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 CND–IS: at least 4 years in network systems and technology CNDSP manager: at least 4 years in CND management	IASAE I: entry level position with 0 or more years of experience IASAE II: at least 5 years of experience IASAE III: at least 10 years of experience
On-the-Job Training Evaluation	No	Yes (only for initial position IAT I)	Yes (except CNDSP manager)	No

Appendix E

Risk Management Framework and DOD 8570.01–M Category and Work Role Comparison

E–1. References

DODI 8510.01 and DOD 8570.01–M compare how each role correlates with the others.

E–2. Work role comparisons

Table E–1 represents the comparison of titles in DODI 8510.01 and DOD 8570.01–M.

Table E–1
Work role comparisons

Risk Management Framework Title	DOD 8570.01–M Category/Level	Training Requirements	Certification Requirements	DOD Cyberspace Workforce Framework Category/Specialty Area	Appointed on Letter?
Senior Information Security Officer	None	Be familiar with CNSSI 1253, DODI 8510.01, and eMASS requirements	None	Oversee Governance-Executive Cyberspace Leadership	Yes
AO	AO	See paragraph 7–3	DOD AO WBT every 3 years	Securely Provision-Risk Management	Yes
AO Designated Representative	AO	See paragraph 7–3	DOD AO WBT every 3 years	Securely Provision-Risk Management	Yes
Security Control Assessor	IAT III or IAM II	See IAT requirement in table D–1 Additional training includes completing the Control Validator training and Security Controls Assessor in eMass (upload certificate in ATCTS)	Yes	Securely Provision-Risk Management	Yes
ISSM	IAM III or IAM II	See IAM requirements in table D–1	Yes (see http://iase.disa.mil/iawip/Pages/iabaseline.aspx)	Oversee Governance-Cybersecurity Management	Yes
ISSO	IAM II or IAM I	See IAM requirements in table D–1	Yes (see http://iase.disa.mil/iawip/Pages/iabaseline.aspx)	Oversee Governance-Cybersecurity Management	Yes
ISO	None	See paragraph 7–4	None	In accordance with job functions	Yes
Not applicable	IASAE I or IASAE II or IASAE III	See IASAE requirements in table D–1	None	Securely Provision or Oversight & Maintain specialty and work role in accordance with job functions	Yes
Not applicable	IAT I/IAT II/IAT III	See IAT requirements in table D–1	Yes (see http://iase.disa.mil/iawip/Pages/iabaseline.aspx)	Operate & Maintain specialty and work role in accordance with job functions	Yes

Table E–1
Work role comparisons—Continued

Risk Management Framework Title	DOD 8570.01–M Category/Level	Training Requirements	Certification Requirements	DOD Cyberspace Workforce Framework Category/Specialty Area	Appointed on Letter?
Not applicable	CNDSP specialty area in DOD 8570.01–M	See CNDSP requirements table D–1	Yes (see http://iase.disa.mil/iawip/Pages/iabaseline.aspx)	Protect & Defend specialty and work role in accordance with job functions	Yes

Appendix F

Resources

F–1. Army Training and Certification Tracking System

ATCTS is located at https://atc.us.army.mil.

F–2. Cybersecurity Fundamentals

Cybersecurity Fundamentals (formerly Information Assurance Fundamentals) is located at https://cs.signal.army.mil (under Courses) or at https://cs.signal.army.mil/iaf/default.asp.

F–3. Skillport

Skillport (Army e-Learning) is located at https://usarmy.skillport.com. All required Skillport training is located under Catalog > CIO–G–6/Cybersecurity IA/IT Training.

Note. Most computing environment training modules are now learning programs. Users must enroll first.

F–4. Federal Virtual Training Environment

FedVTE is located at https://fedvte.usalearning.gov/. New users should self-register.

F–5. MeasureUp

DOD MeasureUp pretest is located at http://dod.measureup.com. First time users must register. These procedures are listed on the ATCTS website under Pre-Assessment Test Information.

F–6. Templates

a. Duty Appointment Letter templates and DA Form 7789 can be found on the ATCTS website under Compliance Information > Documents.

b. Voucher request form is located on the ATCTS website under Documents.

Glossary

Section I

Abbreviations

AKO
Army Knowledge Online

AO
authorizing official

AR
Army regulation

ATCTS
Army Training and Certification Tracking System

AUP
acceptable use policy

CAM
communications account manager

CAP
Certified Authorization Professional

CASP
CompTIA Advanced Security Practitioner

CE
continuing education

CIO
Chief Information Officer

CISA
Certified Information Systems Auditor

CISM
Certified Information Security Manager

CISSP
Certified Information Systems Security Professional

CJCSI
Chairman of the Joint Chiefs of Staff Instruction

CND
computer network defense

CND–A
CND analyst

CND–AU
CND auditor

CND–IR
CND incident responder

CND–IS
CND infrastructure support

CNDSP
computer network defense service provider

CNSSI
Committee on National Security Systems instruction

COCOM
combatant command

CompTIA
Computing Technology Industry Association

COMSEC
communications security

CPA
client platform administrator

CPSO
client platform security officer

DA
Department of the Army

DA Pam
Department of the Army pamphlet

DCWF
DOD cyberspace workforce framework

DD Form
Department of Defense form

DISA
Defense Information Systems Agency

DMDC
Defense Manpower Data Center

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DWC
DOD Workforce Certification

DWCA
Defense Workforce Certification Application

eMASS
Enterprise Mission Assurance Support System

FedVTE
Federal Virtual Training Environment

GIAC
Global Information Assurance Certification

IA
information assurance

IAM
information assurance manager

IASAE
information assurance system architect and engineer

IASE
Information Assurance Support Environment

IAT
information assurance technical

ID
identification

IMO
information management officer

IS
information system

ISACA
Information Systems Audit and Control Association

ISC2
International Information System Security Certification Consortium

ISO
information system owner

ISSM
information systems security manager

ISSO
information system security officer

IT
information technology

KSA
knowledge, skills, and abilities

MTT
mobile training team

PIT
platform information technology

POC
point of contact

WBT
web-based training

Section II

Terms

Authorized user
Any appropriately cleared individual required to access a DOD IS to carry out or assist in a lawful and authorized governmental function. Authorized users include DOD employees, contractors, and guest researchers (see DOD 8570.01–M).

Authorizing official
Senior (federal) official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (see CNSSI 4009).

Certification
Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval, based on a set of standards for a specific profession or occupation's functional job levels. Each certification is designed to stand on its own, and represents an individual's mastery of a particular set of knowledge and skills (see DOD 8570.01–M).

Computing environment
Workstation or server host and its operating system, peripherals, and applications (see CNSSI 4009).

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (see DODI 8510.01).

Cybersecurity service provider
An organization that provides one or more cybersecurity services to implement and protect the DOD information network (see DODI 8530.01).

Enclave
Collection of ISs connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location (see CNSSI 4009).

Information assurance/cybersecurity workforce
The IA workforce focuses on the operation and management of IA capabilities for DOD systems and networks. The workforce ensures adequate security measures and established IA policies and procedures are applied to all ISs and networks. The IA workforce includes anyone with privileged access and IA managers who perform any of the responsibilities or functions described in this pamphlet. The DOD IA workforce includes, but is not limited to, all individuals performing any of the IA functions described in this pamphlet. Additionally, the IA workforce categories, specialties, and their functions are expanded to include system architecture and engineering as well as CND, certification and accreditation, and vulnerability assessment in this pamphlet.

Information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (see CNSSI 4009).

Information system architect
An individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting ISs supporting those missions and business processes.

Information system owner
The ISO is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an IS (see NIST Special Publication 800–37).

Information systems security manager
Individual responsible for the IA of a program, organization, system, or enclave (see CNSSI 4009).

Information technology
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (see CNSSI 4009).

Integrity
The property whereby an entity has not been modified in an unauthorized manner (see CNSSI 4009).

Least privilege
The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function (see CNSSI 4009).

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 that provides for the application of IA controls (see DOD 8570.01–M).

On–the–job training
Supervised hands-on training based on specific performance criteria that must be demonstrated to a qualified supervisor (see DOD 8570.01–M).

Privileged access
An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions. Privileged access typically provides access to the following system controls: access to the control functions of the IS/network, administration of user accounts, and so on; access to change control parameters (for example, routing tables, path priorities, addresses) of routers, multiplexers, and other key IS/network equipment or software; ability and authority to control and change program files, and other users' access to data; direct access to operating system level functions (also called unmediated access) that would permit system controls to be bypassed or changed (see DOD 8570.01–M).

Privileged user
A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform (see CNSSI 4009).

Role–based access control
Access control based on user roles (in other words, a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals (see CNSSI 4009).

System administrator
Individual responsible for the installation and maintenance of an IS, providing effective IS utilization, adequate security parameters, and sound implementation of established IA policy and procedures (see CNSSI 4009).

System security plan
The formal document prepared by the ISO (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan (see CNSSI 4009).