What if I do not become certified within the 6-month window?

Personnel who are not appropriately qualified within 6 months after assignment to a CS position or who fail to maintain their certification status will not be permitted privileged access. Should an account become noncompliant in accordance with DOD 8570.01-M, the Cybersecurity Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR, will instruct the account holder's ISSM or responsible network enterprise center to disable the account until the user becomes compliant.

There are extenuating circumstances that prevented me from becoming certified. May I obtain a waiver?

The authorizing official (AO) may waive the certification requirement under severe operational or personnel constraints. The unit must submit a request for a waiver to the AO stating the reason for the waiver and the plan to eliminate the constraint. Waivers will not extend beyond 6 months, must include an expiration date, and be documented in the individual's CS training record.

How are qualifications tracked that are required by DOD 8570.01-M?

The Army Training and Certification Tracking System (ATCTS) enables managers at all levels to report and manage training and certification of their CS workforce and general users. Baseline certification test vouchers are issued and managed in ATCTS.

Questions? Need more information?

Visit these websites:

AE-ITT
Army in Europe Information Technology Training

United States Army Europe
Information Technology Training
Program
https://itt.eur.army.mil

Information Assurance Program
Management
https://intranet.eur.army.mil/hq/iassure/SitePages/Home.aspx

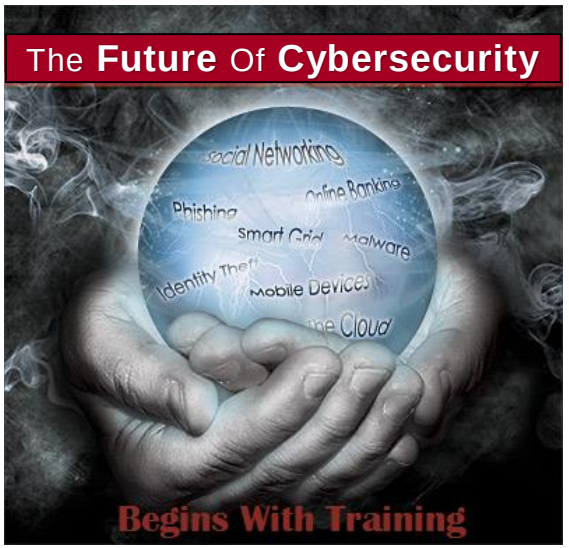
DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Information Assurance Support
Environment
http://iase.disa.mil/

AE Misc Pub 25-2-4 ● 9 July 2015

DOD 8570.01-M Cliff Notes and Key Points

Cybersecurity Division Program Management



"Empowering Cybersecurity Personnel with Knowledge!"

Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command, Europe Region
Sembach, Germany

What is DODD 8570.01?

Department of Defense Directive (DODD) 8570.01 provides guidance and procedures for the training, certification, and management of all Government employees who conduct cyber-security (CS) functions in assigned duty positions. These individuals are required to maintain an approved certification for their particular job classification.

Who is affected by DODD 8570.01?

Military personnel, Department of the Army civilians (DACs), contractors, and local national employees with privileged access to a DOD information system (IS) performing CS functions either full-time, part-time, or as part of their regular duties, regardless of the job or occupational series.

What is the purpose of DODD 8570.01?

The ultimate vision of the directive is a sustained, professional CS workforce that has the knowledge and skills to effectively prevent and respond to attacks against DOD information, information systems (ISs), and IS infrastructures. This effort will enable DOD to put the right people with the right skills in the right positions to protect DOD ISs.

How long do I have to become certified?

No later than 6 months after being assigned to a CS position, all Service personnel, DACs, LN employees, and nonappropriated fund employees must obtain baseline certification. Contractors must have the information assurance (IA) baseline certification required by the CS contract.

Baseline Certification

What do I need?

The table below provides the approved baseline certifications for the CS workforce. Personnel performing CS functions must obtain one of the certifications required for their position category or specialty and level. Refer to appendix 3 of DOD 8570.01-M for further guidance. To obtain the latest certification, visit the Defense Information Systems Agency (DISA) website at *http://iase.disa.mil/iawip/Pages/iabaseline.aspx*.

	IAT Level I	IAT Level II	IAT Level III
	A+-CE Network+CE SSCP CCNA-Security	GSEC Security+CE SSCP CCNA-Security	CISA ~~GSE~~ GCED CISSP *(or Associate)* CASP
	IAM Level I	**IAM Level II**	**IAM Level III**
	CAP ~~GISF~~ GSLC Security+CE	CAP GSLC CISM CASP CISSP *(or Associate)*	GSLC CISM CISSP *(or Associate)*
	IASAE I	***IASAE II***	***IASAE III***
	CISSP *(or Associate)* CASP CSSLP	CISSP *(or Associate)* CASP CSSLP	CISSP-ISSEP CISSP-ISSAP
	CNDSP Analyst	***CNDSP Infrastructure Support***	***CNDSP Incident Responder***	***CNDSP Auditor***	***CNDSP Manager***
	GCIA CEH GCIH	SSCP CEH	GCIH CSIH CEH GCFA	CISA GSNA CEH	CISSP-ISSMP CISM

Computing Environment (CE)

I am an information assurance technical (IAT) or computer network defense (CND) professional. Do I need an operating system (OS) certification in addition to baseline certification?

If you are an IAT or CND professional and have privileged access, you must obtain training for the OS and security-related tools and devices you support as required by your organization. The requirement to be both baseline- and CE-certified is mandated by DODD 8570.01. Unlike baseline certification, the CE certification you require is assigned by your supervisor or information system security manager (ISSM) based on your position's requirements.

Where can I become certified?

DODD 8570.01 and AR 25-2 prescribe training and certification requirements. According to AE Regulation 25-2, the Army in Europe Information Technology Training (AE-ITT) Program is the primary source of information technology (IT) and CS training for Army in Europe personnel. All USAREUR major subordinate and specialized commands and all United States Army garrisons (USAGs) are required to use the AE-ITT Program as the primary source for all instructor-led IT and CS training. The Government will not fund the training and certification of contractors.