

DoD Directive 8570.1

Department of Defense Directive 8570.1

In 2004, the US Department of Defense (DoD) established Directive 8570.1: Information Assurance Training, Certification and Workforce Management. It requires that all DoD Information Assurance technicians and managers are trained and certified to effectively defend DoD information, information systems and information infrastructures.

CompTIA Certifications for D8570.1

The DoD Directive 8570.1 Implementation Manual has an approved list of certifications to meet the DoD D8570.1 requirements; [CompTIA A+](#), [Network+](#) and [Security+](#) are included. CompTIA certification programs receive worldwide use and recognition, and are built with the knowledge of industry leaders from the public and private sectors, including training, academia and the government. CompTIA certifications also serve as the building blocks for more advanced certifications, and are accepted as pre-requisites or electives for higher-level certifications such as MCSA, Novell's CNE (Netware 5) and ISACA.

How quickly does the DoD expect its personnel to obtain certification?

DoD officials plan to have all affected personnel certified over a four-year period by reaching a 10% minimum certified in fiscal year 2007 and 30% certified per each fiscal year thereafter.

How does the mandate impact contractors doing business with DoD?

DoD officials recently added a clause to the Defense Federal Acquisition Regulation Supplement (DFARS) that will require any company bidding on new DoD information technology (IT) contracts to have 8570-compliant personnel. The agency is currently asking for public comment on the clause, though a few requests for proposals (RFPs) and requests for quotes (RFQs) are already incorporating the new language. Industry observers expect the new clause to take full effect in summer 2007.

What is the significance of this mandate and of commercial certification in general?

This mandate will have far-reaching implications, including:

- The Directive is viewed as a government endorsement of the effectiveness and cost-efficiency of commercial certification.
- It provides military and civilian personnel with a certification that is professional, internationally recognized and vendor-neutral (not tied to any agency, technology or product).
- It provides a portable certification that is recognized in both the public and private sectors.
- It mandates and endorses a global standard (ANSI/ISO/IEC 17024).
- It positions the information security profession as a distinct job series.

What current challenges will enterprise-wide certification address?

By providing an objective measure of the quality of knowledge, skills, and abilities that each employee possesses and a way to standardize this measurement, enterprise-wide certification:

- Eliminates consistency issues and problems caused by the lack of regulated internationally recognized qualifications.
- Provides a metric that can be easily and reliably measured.
- Provides intangible benefits such as renewed motivation, diligence, and leadership.

- Encourages personnel to upgrade their education and skills -- and keep those skills current through continuing professional education.
- Creates professional pride through recognition of an accepted global standard.
- It reduces the language disparity between those who determine and write information security policy and those who implement it.

Are there different certification requirements for managers than for technically oriented information assurance or information security personnel?

Yes. There are six categories outlined in the Directive matrix with different roles and responsibilities and different certifications applicable for each category. Information assurance personnel must be certified under a credential that meets the criteria laid out in these six matrix categories. Managers must meet the certification requirements outlined under the Technical III (T3) and all Management categories (M1, M2, and M3). Technical personnel must meet the certification requirements outlined under the Technical I (T1) and Technical II (T2) categories (Visit www.isc2.org/dodmandate or reference matrix below.) The DoD 8570.1M Manual states that additional certifications will be added in the future.

IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA CISSP GSE SCNA
IAM Level I	IAM Level II	IAM Level III
GISF GSLC Security+	GSLC CISM CISSP	GLSC CISM CISSP

DoD 8570.01-M, Table AP3.T2. DoD Approved Baseline Certifications

References to the DoD 8570.1M are from:

(ISC)²® Website <https://www.isc2.org/cgi-bin/content.cgi?page=949>

CompTIA Website http://certification.comptia.org/resources/US_Gov.aspx