



COMDTINST 5200.3  
MARCH 23, 2010

COMMANDANT INSTRUCTION 5200.3

Subj: INFORMATION ASSURANCE PROFESSIONAL CERTIFICATIONS

Ref: (a) DHS Sensitive Systems Policy Management Directive 4300A, DHS MD 4300.1  
(b) DHS Information Technology Security Essential Body of Knowledge, ITSEC EBK  
(c) Information Assurance Workforce Improvement Program, DOD 8570.01-M

1. PURPOSE. To establish policy and identify certification standards for Information Assurance (IA) professionals based on roles held within the Coast Guard.
2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements shall comply with the provisions of this instruction. Internet release is authorized.
3. DIRECTIVES AFFECTED. None.
4. DISCUSSION. The Coast Guard has adopted applicable segments of references (a), (b), and (c) to form the basis for certifying IA professionals. By ensuring individuals in IA roles possess appropriate industry standard certifications the Coast Guard will be prepared to create, maintain, and safeguard information for all mission and administrative activities.
5. POLICY.
  - a. General.
    - (1) Commandant (CG-6) establishes the role-based industry standard certifications for Information Assurance (IA) professionals in significant information security roles. An IA professional is defined as a person who has an active user or administrative account on any CG network, information system, or contractor network with CG network access and is designated to perform an IA role within the CG enterprise.

DISTRIBUTION – SDL No. 155

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1	1	1	1	1		1	1		1	1	1	1	1	1		1		1					
B		8	10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1		1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
E	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		1		1	1			1	1		
F																	1	1	1							
G		1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

- (2) Commandant (CG-6) shall identify all IA professionals based on their role and functions, and then use this instruction to determine the applicable industry standards and certifications to fulfill IA duties. A roster shall be maintained by units to identify IA personnel. Certifications must be recorded in Direct Access (DA) for all government and military personnel who fill an IA role.
  - (3) Contractor certifications must be recorded and maintained by the Contracting Officer's Technical Representative (COTR). The following items shall be recorded:
    - (a) The total number of IA personnel that have received role-based certification preparation or Continuing Professional Education (CPE) credits.
    - (b) IA personnel that have achieved IA Professional Certification, the title of the certification, the date of completion, and the cost.
  - (4) CG units or division managers shall forecast IA certifications for the upcoming FY and submit plans to Commandant (CG-6) prior to beginning of Q1 of upcoming FY.
  - (5) CG members and contractor employees with significant security responsibilities (e.g., ISSO's, system administrators) shall receive initial professional certification preparation, and annual continuing professional education thereafter, specific to their security responsibilities prior to being granted access to CG IT systems to perform those assigned security duties.
6. CERTIFICATION CATEGORIES AND TIERS. The IA roles described previously can be separated into two categories: Information Assurance-Technical (IAT) and Information Assurance-Managerial (IAM) as defined by reference (c). Within each category, there are three tiers of certification (I, II and III). A person's role and function provide the basis for determination of the certification category and tier.
- a. Each person filling an IA role must be measured against the IA competencies defined in paragraph 7 to determine the certification requirements.
  - b. A position may span multiple certification categories and tiers. In such an event, the member must meet the certification requirements of the highest tier.
  - c. Certification categories and tiers do not necessarily relate to pay grade on a one-to-one basis.
7. IA COMPETENCIES. IA competencies will be created for each category and tier. These IA competencies will become requirements to the appropriate IA positions. As a person completes the certification requirements set forth for various competencies, evidence must be provided to administrative personnel (e.g. unit Training Office) to have the certifications added to the member's record. The six IA competencies are defined as the following.
- a. Information Assurance Technical (IAT).
    - (1) IAT Tier I (IAT1) personnel will:
      - (a) Usually possess zero to four years of experience in a related IA position.

- (b) Possess basic knowledge of IA concepts, practices, and procedures.
- (c) Only perform actions that are authorized and directed by approved policies and procedures.

(2) IAT Tier II (IAT2) personnel will:

- (a) Usually possess three to seven years of experience in a related IA position.
- (b) Possess a mastery of the requirements at the IAT1 level.
- (c) Apply knowledge and experience with IA concepts, practices, and procedures.

(3) IAT Tier III (IAT3) personnel will:

- (a) Usually possess a minimum of seven years of experience in related IA positions.
- (b) Possess a mastery of the requirements at the IAT1 and IAT2 levels.
- (c) Apply extensive knowledge of IA concepts, practices, and procedures to ensure the successful operation, management, and security of the systems under their control.
- (d) Work independently to resolve issues effectively and may manage IAT1 and IAT2 level personnel.

b. Information Assurance Managerial (IAM).

(1) IAM Tier I (IAM1) personnel will:

- (a) Usually possess zero to five years of IA management experience.
- (b) Apply IA knowledge of policies and procedures to develop, implement, and maintain their system(s) within their assigned environment.

(2) IAM Tier II (IAM2) personnel will:

- (a) Usually possess a minimum of five years of IA management experience.
- (b) Apply IA knowledge of policies and procedures to develop, implement, and maintain all systems within their assigned environment.

(3) IAM Tier III (IAM3) personnel will:

- (a) Usually possess a minimum of ten years of IA management experience.
- (b) Apply IA knowledge of policies, procedures, and workforce infrastructure to develop, implement, and maintain their assigned environment.

8. ROLES. The following are descriptions of the IA professional roles that require industry standard certifications:

a. Chief Information Officer (CIO, Commandant (CG-6)) (IAM3).

- (1) Promulgates and monitors the implementation of the CG information security strategy. Ensures alignment with DHS/DoD strategy. Is responsible for the strategic use and management of CG information, information systems, and information technology (IT).
- (2) Establishes and oversees IT security program, including evaluation of compliance with the Department of Defense (DoD), Department of Homeland Security (DHS) and CG policies and the effectiveness of policy implementation.
- (3) Leads the evaluation of new and emerging IT security technologies.

b. CG Chief Information Security Officer (CISO, Commandant (CG-65)) (IAM3).

- (1) Drafts, maintains, and executes in the CG information security strategy.
- (2) Develops and enforces CG information security policies, procedures and metrics, security awareness program, business continuity and disaster recovery plans, and responds to emerging industry and governmental IA compliance challenges.

c. Information Systems Security Manager (ISSM, Commandant (CG-651)) (IAM3).

- (1) Responsible for overseeing, evaluating, and supporting IA compliance.
- (2) Monitors and evaluates emerging information security threats.
- (3) Performs a variety of activities, encompassing compliance with applicable laws and regulations from an internal and external perspective. Activities include leading and conducting internal investigations, assisting employees' compliance with CG information assurance, information systems, and telecommunications policies and procedures, and serving as a resource to external compliance officers during independent assessments.
- (4) Provides guidance and independent evaluation of information systems and infrastructure to CG, DHS, and DoD leadership.
- (5) Provides policy interpretation, guidance, and direction to CG IA personnel.
- (6) Oversees the implementation of this instruction and its requirements by CG units and division managers.
- (7) Reviews and approves CG Information System Security Certification Plans.

d. Certification Authority (CA) (IAM3).

- (1) Comprehensively evaluates the information security of an Information System (IS), General Support System (GSS) including Local Area Network (LAN), and Major Application (MA).
  - (2) Determines whether the security controls evaluated meet published enterprise requirements for that system or similar systems.
  - (3) Determines whether adequate Contingency Plans (CP) are in place, have been regularly tested, and are recorded in the correct format.
  - (4) Determines whether the risks surrounding the use of the system are adequately addressed, remediated, or identified and a recommendation for or against an Authority to Operate (ATO) is granted by the Designated Approving Authority (DAA).
- e. CG Computer Incident Response Team (CGCIRT) (IAT3 / IAM2).
- (1) Performs a variety of highly technical analyses and procedures in collecting, processing, preserving, analyzing, and presenting computer-related evidence, including, but not limited to, data retrieval, breaking passwords, and finding hidden or otherwise “invisible” information.
  - (2) Provides detailed reports to DHS Security Operations and Network Operations Centers (SOC and NOC, respectively).
  - (3) Researches and implements applicable patches including Information Assurance Vulnerability Alerts (IAVA), vulnerability bulletins, and technical advisories for CG IT systems.
  - (4) Analyzes CG IT systems and implements security countermeasures as necessary.
  - (5) Analyzes patterns of noncompliance and takes appropriate action to minimize the impact upon CG IT systems.
- f. IT Security Engineer (IT System Developer) (IAT3).
- (1) Applies cross-disciplinary IT security knowledge to build IT systems that remain dependable in the face of malice, error, and mischance.
  - (2) Develops and applies access controls and other security measures to their IT system throughout the various milestones of the System Development Life Cycle (SDLC).
  - (3) Establishes security test plans and procedures for IT systems IAW the National Institute of Standards and Technologies (NIST) and other industry best practices.
  - (4) Conducts tests of safeguards in accordance with developed test plans and procedures for IT systems.
  - (5) Responsible for the security of the data contained within their system and the end-to-end transmission of the data (if applicable).

(6) Responsible for developing recommended maintenance tasks and schedules for maintaining the integrity of their system.

g. Information Systems Security Officer (ISSO) (IAT2-3 / IAM2).

(1) Concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability for their area of responsibility (AOR) or for their system(s).

(2) Coordinates with IT Technical Support Personnel, CGCIRT, and ISSM to resolve IA problems.

(3) Participates in the Certification and Accreditation process for the CG IT systems within their AOR.

(4) Recognizes possible security violations and takes appropriate actions to report the incident and forward corrective action requests to the IT Support Professionals or to CGCIRT, as appropriate.

(5) Manages corrective action when an IA incident or vulnerability is discovered within their AOR.

h. IT Technical Support Personnel (IAT1-3).

(1) Ensure the security of information, network systems, and information systems during the Operations and Maintenance phase of the SDLC.

(2) Responsible for the operations and maintenance of CG information systems.

(3) Recognize potential or actual security violations, report incidents to the ISSO, and take action as directed.

(4) Provide physical or intellectual forensic evidence to the ISSO upon direction.

(5) Provide end user support for CG IT hardware and software.

(6) Provide direction and advice to users for the procurement of new hardware or software.

(7) Support, monitor, test, and troubleshoot hardware and software installations and problems with CG IT systems.

(8) Manage user accounts, rights, and access to CG IT systems.

(9) Include, but not limited to, help desk support personnel, systems, database, and network administrators.

9. **REQUIRED CERTIFICATIONS.** All CG IA professionals shall achieve, manage, and maintain certain certifications to adequately perform their jobs. Table 1 identifies the industry standard certifications that satisfy the competency requirements set forth by this instruction.

- a. Only one industry certification is required to satisfy a given competency. (Note: Some certifications satisfy multiple competencies.)
- b. All military personnel currently assigned to an IA position shall obtain the required certification for their position within twelve months of the date of this instruction. All government employees currently assigned to an IA position shall be granted a waiver for the required certification within twelve months of the date of this instruction. Military personnel and government employees assigned to an IA position after the date of this instruction shall obtain the required certification for their position within twelve months of their check-in date or date of hire.

Table 1: IA Professional Certification Matrix

Information Assurance Technical (IAT)		
IAT1	IAT2	IAT3
A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA CISSP GSE SCNA
Information Assurance Managerial (IAM)		
IAM1	IAM2	IAM3
GISF GSLC Security+	GSLC CISM CISSP	GSLC CISM CISSP

c. **Certifications.** The explanation of each industry standard certification is available at the identified provider’s web site.

- (1) A+ is provided by Computing Technology Industry Association (CompTIA). The A+ certification validates the latest skills needed by today's computer support professionals. The certification confirms a technician's ability to perform tasks such as installation, configuration, diagnosing, preventive maintenance and basic networking.
- (2) Certified Information Security Auditor (CISA) is provided by ISACA. The CISA certification signifies the professional commitment to serving an organization and the IA audit, control and security industry with distinction.
- (3) Certified Information Security Manager (CISM) is provided by Information Systems Audit and Control Association (ISACA). The Certified Information Security Manager (CISM) certification is a unique management focused certification for the member who manages, designs, oversees and assesses an enterprise's information security program.

- (4) Certified Information Systems Security Professional (CISSP) is provided by the International Information Systems Security Certifications Consortium (ISC)<sup>2</sup>. The CISSP is designed for IA professionals who must demonstrate a working knowledge of information security and confirm commitment to their profession.
- (5) GIAC Information Security Fundamentals (GISF) is provided by SANS Institute. The GISF certification is designed IAM1 personnel who write, implement, or adhere to policy, disaster recover or business continuity and need an overview of risk management and defense in depth techniques.
- (6) Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC) is provided by the System Administration, Networks, and Security (SANS) Institute. The GSEC certification is designed for IAT personnel that want to fill the gaps in their understanding of technical information security and demonstrate they are qualified for hands on roles with IT systems with respect to security tasks.
- (7) GIAC Security Expert (GSE) is provided by SANS Institute. The GSE certification is designed for IAT3 personnel and the completion of this certification promises the holder possess significant skills in the following areas: Intrusion detection and traffic analysis, incident handling, Windows security, secure communications, communication protocols, and security policy creation and analysis.
- (8) GIAC Security Leadership Certificate (GSLC) is provided by SANS Institute. The GSLC certification is designed for IAM personnel and offers a comprehensive coverage of security technology with a focus on the management application, with leadership and organizational tips.
- (9) Network+ is provided by CompTIA. The Network+ certification validates the knowledge and skills of networking professionals. The certification confirms a technician's ability to describe the features and functions of networking components and to install, configure and troubleshoot basic networking hardware, protocols and services.
- (10) Security+ is provided by CompTIA. The Security+ certification validates the member's knowledge of communication security, infrastructure security, cryptography, operational security, and general security concepts.
- (11) Security Certified Network Architect (SCNA) is provided by Security Certified Program. The SCNA certification focuses on the advanced security skills and technologies of building trusted networks, including: Law and legislation issues, forensics, wireless security, securing e-mail, biometrics, digital certificates and digital signatures, PKI policy and architecture, and cryptography.
- (12) Security Certified Network Professional (SCNP) is provided by Security Certified Program. The SCNP certification validates the essential security skills for securing strategic elements of the network, including: Analyzing packet signatures, creating security policies, performing the risk analysis, Internet security, cryptography, and hardening Windows Server 2003.

(13) System Security Certified Practitioner (SSCP) is provided by (ISC)2. The SSCP is especially designed for network and systems administrators who implement policies, standards, and procedures on the various hardware and software programs for which they are responsible.

10. WAIVERS. Waivers for these requirements may be submitted to the ISSM in the form of official CG Memorandum. Waivers will be evaluated for reasons including, but not limited to the following:

- a. Time. If a member does not satisfy the experience requirements of a given certification, then a waiver may be granted for the duration of the remaining experience requirement duration.
- b. Unsuccessful Exam Completion. If a member is unable to complete a certification exam after the three CG-funded attempts, then a waiver may be granted.
- c. Contractual Limitations. If a member cannot be obligated under an existing contract to obtain a required certification, a waiver may be granted.
- d. Temporary Duty. If a member is only assigned the position for a short duration or is temporarily performing those job functions until the position is filled by another individual.
- e. All existing CG employees will be granted waivers for the requirements set forth in this instruction. All new CG employees shall satisfy the requirements set forth in this instruction.

11. TRAINING SOURCES.

- a. Online Web-Based Courses. Multiple no-cost online web-based preparation courses are available for each certification identified in Table 2.
  - (1) Free online web-based training through SkillSoft.
  - (2) Free online web-based training for users with a valid "uscg.mil" e-mail address can utilize Carnegie Mellon's Virtual Training Environment (<http://www.vte.cert.org/vteweb>).
  - (3) Some training providers also provide online web-based preparation courses for a fee; these courses offer online tutoring, test preparation, chat capabilities with instructors (not to be utilized on the CG Standard Workstation.) Funding for these courses will be at the discretion of the member's unit.
- b. Resident Courses. Multiple resident course providers are available world-wide for the certifications. Funding for these courses will be at the discretion of the member's unit.

12. TESTING SITES. Many testing sites are available world-wide for completing the certification exams. Members are expected to choose a site within the normal commuting distance to prevent the need to utilize a travel order to complete the exam.

13. FUNDING.

- a. Military Personnel and Government Employees. Certification test and certification maintenance fees for military personnel and government employees may be funded by the member's unit and/or Commandant (CG-6), subject to availability of funds. Each member will be afforded three opportunities to pass a single certification exam. Each member must wait a minimum of 30 days between testing attempts at a particular certification exam. Military personnel will incur one year of obligated service from the date of last certification exam attempt. Only one professional certification exam and the applicable annual maintenance fee for the IA position held may be funded by the Coast Guard. Additional professional certification costs are the responsibility of the member. For example, a member holds two certifications (CISM and CISSP) while in an IA position requiring an IAM3 competency, only one certification and fee will be funded by the Coast Guard.
- b. Contractor personnel. Contractors will be held to the same industry standards and certification requirements; however, it is their responsibility to fund their own training and certifications. The training and certification requirements shall be added to all future statements of work and awarded contracts.

14. MAJOR CHANGES. This is the initial release of this instruction; therefore this section is not applicable.

15. REQUESTS FOR CHANGES. Units and individual members may recommend changes in writing via the chain of command to:

COMMANDANT (CG-6)  
U S COAST GUARD  
2100 2<sup>ND</sup> ST SW STOP 7101  
WASHINGTON DC 20593-7101

16. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATION. Environmental considerations were examined in the development of this instruction and determined to not be applicable.

17. FORMS/REPORTS: The forms referenced in this Instruction are available in USCG Electronic Forms on the Standard Workstation or on the Internet: <http://www.uscg.mil/forms/>; CGPortal at <https://cgportal.uscg.mil/delivery/Satellite/uscg/References>; and Intranet at <http://cgweb.comdt.uscg.mil/CGForms>.

M. B. LYTLE /s/  
Acting Commandant for Command,  
Control, Communications, Computers, and  
Information Technology