



**NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 6-34**



Issue Date: 30 August 2010
Revised: 17 July 2015

POLICY STATEMENT

**COMPLIANCE WITH DOD INFORMATION ASSURANCE
WORKFORCE IMPROVEMENT PROGRAM**

1. The [NSA/CSS Global Cryptologic Enterprise \(GCE\)](#) employs personnel who perform a wide variety of [information assurance \(IA\)](#) roles and functions, in order to protect its information and network resources. This policy implements the Department of Defense (DoD) IA Workforce Improvement Program (WIP), a program to provide IA professionals with a common set of IA skills and knowledge through a training and certification program.

2. In an effort to better manage the IA workforce, maximize its effectiveness, and comply with DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," and its associated Manual ([References a and b](#)), the NSA/CSS [Mission Resource Authorities](#) shall:


a. With the assistance of the [NSA IA Workforce Improvement Program Office](#) of Primary Responsibility (IA WIP OPR), identify and catalog their [Information Assurance Workforce](#) positions in terms of IA category, specialty, and level as defined in [Reference b](#);

b. Require employees working in IA positions to provide evidence of their current certifications and experience for entry into the IA WIP database. For instructions on registering IA WIP certification and renewal information, contact the [NSA IA WIP OPR](#);

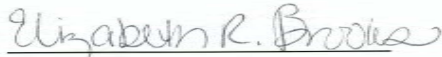
c. Require supervisors to verify that employees occupying identified IA billets are appropriately certified and to meet with them to plan appropriate training and certification exams required to achieve IA WIP compliance ([References b and c](#)), and incorporate these objectives in Individual Development and Individual Training Plans as applicable; and

d. Ensure that supervisors and training authorities work together to provide training requirements to Associate Directorate for Education and Training (ADET) based on information in the Human Resources Management System (HRMS) database.

3. This policy applies to all [affiliates](#) and to contractors for whom specific contractual provisions apply regarding IA training and certification ([Reference d](#)).



KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS



Endorsed by
Associate Director for Policy

DISTRIBUTION:

TS23
DJ1

This Policy 6-34 supersedes Annex O of NSA/CSS Manual 130-1, “Information System Security Training Requirements,” dated September 2001. An administrative update was approved on 21 May 2012 to clarify that this Policy supersedes Annex O of NSA/CSS Manual 130-1, update hyperlinks, and make other administrative changes. The Chief, Corporate Policy approved an administrative update on 15 October 2013 to update organizational designators and references and repair broken links. The Chief, Corporate Policy approved an administrative update on 4 March 2015 to update the definition of “affiliates” and again on 17 July 2015 to change the overall classification from U//FOUO to UNCLASSIFIED and to approve this policy for public release.

OPI: Information Assurance Workforce Improvement Program Office of Primary Responsibility, TS23, DL iawip_nsa.

No section of this document shall be released without approval from the Office of Corporate Policy (DJ1).

REFERENCES

4. Reference:

a. [DoD Directive 8570.01](#), “Information Assurance Training, Certification, and Workforce Management,” dated 23 April 2007.

b. [DoD 8570.01-M](#), “Information Assurance Workforce Improvement Program,” dated 24 January 2012.

c. [Comptroller Decision Memorandum No. 01-2012](#), “Reimbursement for Professional Certifications, Licenses, and Related Expenses,” dated 23 November 2011.

d. [Defense Federal Acquisition Regulation Supplement, Subpart 239.71](#), “Security and Privacy for Computer Systems,” revised 21 June 2010.

DEFINITIONS

5. Affiliates – A person employed by, detailed to, assigned to, integrated with, or a tenant of a facility within the Global Cryptologic Enterprise and granted access to the enterprise information technology infrastructure for which Director, NSA/Chief, CSS has operational information system security responsibility. This includes, but is not limited to, U.S. Government employees, Service Cryptologic Component personnel, contractors, consultants, and foreign national partners. (Source: [NSA/CSS Corporate Policy Glossary](#))

6. Information Assurance – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Source: [CNSS Instruction 4009](#))

7. Information Assurance 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 information systems and networks. The IA workforce includes anyone with [privileged access](#) and IA managers who perform any of the responsibilities or functions described in Chapters 3-5, 10, or 11 of [Reference b](#). Additionally the IA workforce categories, specialties, and their functions include system architecture and engineering, computer network defense, certification and accreditation, and vulnerability assessment. These individuals are considered to have significant security responsibilities and must receive specialized training and certifications that are monitored and reported per [Reference a](#). (Source: Derived from [Reference b](#))

8. Mission Resource Authorities – They are the Signals Intelligence Director; the Information Assurance Director; the NSA/CSS Chief of Staff; the Technology Director; and the Research Director.

9. NSA/CSS Global Cryptologic Enterprise (GCE) – NSA/CSS worldwide personnel, systems, and facilities:

a. NSA/CSS Headquarters – Primary location of the NSA/CSS Senior Leadership Team;

b. NSA/CSS Washington (NSAW) – NSA/CSS facilities at the Fort Meade, Friendship Annex (FANX), and associated campuses [Finksburg, Kent Island, and all leased facilities in the Baltimore/Washington metropolitan area]; and

c. NSA/CSS Extended Enterprise – NSA/CSS personnel, systems, and facilities at locations other than NSAW. (Source: [NSA/CSS Corporate Glossary](#))

10. 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:

- a. Access to the control functions of the information system/network, administration of user accounts, etc.;
- b. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software;
- c. Ability and authority to control and change program files, and other users' access to data;
- d. Direct access to operating system level functions (also called unmediated access) that would permit system controls to be bypassed or changed; and
- e. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations. ([Reference b](#))