CNSS Directive No. 500
August 2006

Information Assurance (IA)
Education, Training, and Awareness

This document prescribes minimum standards. Your department or agency may require further implementation.

CNSS Directive No. 500
August 2006

Committee on National Security Systems

Chair

FOREWORD

1. The *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 5 July 1990, assigns to the CNSS a key responsibility for ensuring the development and implementation of a comprehensive approach for the protection of U.S. Government national security systems and the information they store, process, or transmit. The success of this effort depends not merely on the technical implementation of policies, but also on the vulnerable interface between humans and information systems. Education, training and awareness (ETA) are countermeasures that effectively reduce the human-related risks. To maximize the overall protection of systems and information, it is essential to have a federal work force that is aware of, trained on, and educated about information assurance (IA).

2. This Directive is issued in response to national policy and establishes the requirement for federal departments and agencies to develop and implement IA education, training and awareness programs.

3. Additional copies of this Directive may be obtained from the Committee on National Security Systems (CNSS) website at www.cnss.gov or by contacting the CNSS Secretariat at the address below.

/s/
John G. Grimes

INFORMATION ASSURANCE (IA) EDUCATION, TRAINING AND AWARENESS

SECTION I – PURPOSE

1. This Directive establishes the requirement for federal departments and agencies to establish and implement information assurance (IA) education, training and awareness (ETA) programs for personnel who access, operate, manage, maintain, secure, develop, acquire, *etc.*, National Security Systems (NSS).

SECTION II – SCOPE AND APPLICABILITY

2. This Directive is applicable to all departments and agencies of the U.S. Government, its employees, and contractors, who access, operate, manage, maintain, secure, develop, acquire, *etc.*, national security systems operated by or on behalf of the Federal Government to store, process, or transmit national security information. Additionally, nothing in this Directive shall alter or supersede the existing authorities of the Director of National Intelligence.

SECTION III – AUTHORITY

3. This Directive is issued pursuant to *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 5 July 1990, which mandates the development and implementation of a comprehensive approach to protect U.S. Government NSS. It also supersedes *NSTISS Directive No. 500, Telecommunications and Automated Information Systems Security Education, Training and Awareness*, dated 25 February 1993.

IV – DEFINITIONS

4. Definitions for terminology used in this Directive may be found in *CNSS Instruction (CNSSI) No. 4009, National Information Assurance (IA) Glossary*.

SECTION V – RATIONALE AND OBJECTIVES

5. The evolution of information processing technologies has enabled the Federal Government to store, process, and transmit unprecedented amounts of information. The use of information systems by the Federal Government has focused attention on the need to ensure that these assets (*i.e.*, hardware, software, and firmware) and the information they store, process, or transmit are protected. Information systems must protect the ability of federal departments and agencies to effectively and accurately perform official functions. The responsibility for securing

information and the systems on which it is processed lies with the head of the federal department or agency to whom the information and resources are entrusted.

6. The objective of this Directive is threefold, *viz.*,

a. To require the implementation of programs enhancing the awareness of all persons of the need to protect information as well as systems resources and capabilities;

b. To enhance the public's confidence in the Federal Government's ability to provide information systems protection; and

c. To promote the protection of information and information systems through ETA programs that promote the uniform and consistent understanding of IA principles and concepts.

SECTION VI – POLICY

7. Information Assurance ETA activities are required for all employees and contractors who access, operate, manage, maintain, secure, develop, acquire, etc., a NSS. Such a comprehensive effort must meet the varying levels of knowledge, experience, and responsibilities of employees and contractors, as well as addressing the specific needs of individual departments and agencies. There are certain messages that need to be conveyed to both senior leadership and the workforce:

a. Organizations critically rely on the integrity of the information and availability of information system resources to meet mission requirements.

b. The organization's management is pro-actively committed to protecting information and information system resources.

c. There are consequences for inadequately protecting the organization's information systems' resources.

d. The employee is the key to a successful protection program.

SECTION VII – RESPONSIBILITIES

8. Each federal department and agency will:

a. Fund, develop, and implement an IA ETA program in accordance with the National Manager guidelines and federal requirements.

b. Require in contract language that contractors comply with the provisions of this Directive whenever they access, operate, manage, maintain, secure, develop, acquire, *etc.*, NSS. For contractors, the terms of the contract shall specify this requirement.

c. Ensure all training activities pursuant to the requirements of this Directive are compliant with CNSS standards and guidance and are conducted by individuals who are well-versed in IA concepts and their applications.

9. Every IA ETA program will contain three types of activities: initial awareness orientation, more advanced education and training commensurate with duties and responsibilities, and annual reinforcement activities.

10. The National Manager will:

a. Establish, develop, and implement IA ETA program guidelines in concert with the national security community.

b. Ensure the development of ETA materials based on CNSS IA standards and guidance.

c. Provide guidance to federal departments and agencies in developing and conducting IA ETA activities, as requested.

d. Develop national IA ETA standards and materials and review them annually for currency and relevancy.

e. Encourage federal departments and agencies to develop plans of instruction mapping to CNSS standards.

f. Coordinate with OMB to gather national security system-related IA ETA data reflecting adherence to CNSS Instructions *via* annual FISMA reports.

g. Brief the Committee annually on the status of department and agency CNSSI-compliant IA activities. Metrics, as reported through FISMA, will reflect number of people trained by type of activity, *viz.*, ETA.