

NSTISSD No. 501
16 November 1992


NSTISS
NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY



NATIONAL TRAINING PROGRAM
FOR
INFORMATION SYSTEMS SECURITY
(INFOSEC) PROFESSIONALS

NSTISSC

NATIONAL SECURITY
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY COMMITTEE

CHAIRMAN

FOREWORD

1. The "National Policy for the Security of National Security Telecommunications and Information Systems," signed by the President on July 5, 1990, mandates the development and implementation of a comprehensive approach to national security telecommunications and automated information systems security. It is recognized that the community of information systems security (INFOSEC) professionals has evolved beyond the need for cross-training (i.e., communications security to computer security and vice versa), into a more global concern for the development of a common body of knowledge. This directive is issued in response to those requirements for the training of INFOSEC professionals.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this directive from:

Executive Secretariat
National Security Telecommunications and
Information Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000

3. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

/s/

DUANE P. ANDREWS

**NATIONAL TRAINING PROGRAM FOR
INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS**

SECTION I - PURPOSE

1. This directive establishes the requirement for federal departments and agencies to implement training programs for information systems security (INFOSEC) professionals. For the purpose of this directive, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each phase of the life cycle.

SECTION II - SCOPE AND APPLICABILITY

2. This directive is applicable to all departments and agencies of the U.S. Government, their employees, and contractors who are responsible for the security oversight or management of national security systems during each phase of the life cycle.

SECTION III - AUTHORITIES

3. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988, requires mandatory periodic training for all persons involved in management, use, or operation of federal computer systems that contain sensitive information.

4. National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990, mandates the development and implementation of a comprehensive approach to national security telecommunications and automated information systems security.

5. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992.

SECTION IV - DEFINITIONS

6. The following definitions, applicable to this instruction, are contained in NSTISSI No. 4009, and are listed below for information purposes:

a. Information systems security (INFOSEC) - the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

b. Information systems - any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice and/or data, and includes software, firmware, and hardware.

c. National security systems - those telecommunications and automated information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in 10 U.S.C. Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

d. Telecommunications - the preparation, transmission, communication, or related processing of information (writing images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

e. Telecommunications and automated information systems security - protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information.

SECTION V - RATIONALE AND OBJECTIVES

7. Technology that supports national security systems continues to be enhanced. Integration of telecommunications and automated information systems is commonplace, often obscuring what was once two distinct disciplines. The telecommunications manager's reliance on automated information systems will continue to increase just as will the automated information systems manager's reliance upon telecommunications. As the degree of overlap fluctuates between the two, understanding operational requirements becomes more-difficult. A sharing of knowledge between the two disciplines will ensure that the requirements of both are fully addressed.

8. The objective of this directive is to require the implementation of a training program to provide INFOSEC professionals with a common body of knowledge encompassing both communications security and computer security. Persons who are responsible for the security oversight or management of national security systems, without a basic, yet broad perception of both disciplines, place the systems at risk.

SECTION VI - INFOSEC TRAINING

9. INFOSEC is multidisciplinary in nature, requiring a wide spectrum of knowledge such as operations security, emanations security, physical security, personnel security and related security areas. Recognizing the convergence of traditional telecommunications and automated information systems technology and their growing interdependence, it is necessary to ensure that the work force makes this transition. Basic INFOSEC awareness, training, and education are security countermeasures.

SECTION VII - RESPONSIBILITIES

10. The heads of federal departments and agencies will:

a. Implement an INFOSEC training program as part of the overall training program, in accordance with agency or department specific requirements, following the minimum course content.

b. Ensure that INFOSEC professionals are trained in a common body of knowledge as outlined by the National Manager.

c. Require contractors to comply with the provisions of this directive when they are responsible for the security oversight or management of national security systems, operated by or on behalf of the Federal Government. For contractors, the terms of the contract shall specify this requirement.

11. The National Manager will:

a. Develop and define minimum training standards for an INFOSEC training program.

b. Provide minimum training standards for an INFOSEC program to federal departments and agencies, to include their contractors.

c. Ensure that appropriate INFOSEC training course(s) are developed and include policies, standards, criteria, products, and technologies that result from federal or federally sponsored efforts.

d. Assist other federal departments and agencies in developing and/or conducting INFOSEC training activities, as requested.