AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(k) A senior administrative law judge will be paid by the employing agency the current rate of pay for the level at which the duties to be performed have been placed and at the lowest rate of the level that is nearest (when rounded up) to the highest previous grade and step, or level and rate, attained as an administrative law judge before retirement. An amount equal to the annuity allocable to the period of actual employment will be deducted from his or her pay and deposited in the Treasury of the United States to the credit of the Civil Service Retirement and Disability Fund.

[52 FR 32403, Sept. 10, 1987, as amended at 56 FR 6210, Feb. 14, 1991]

Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems

AUTHORITY: 40 U.S.C. 759 note.

SOURCE: 56 FR 63403, Dec. 4, 1991, unless otherwise noted.

§ 930.301 Definitions.

(a) The amount and type of training different groups of employees will receive will be distinguished by the following knowledge levels identified in the Computer Security Training Guidelines developed by the National Institute of Standards and Technology:

(1) *Awareness level training* creates the sensitivity to the threats and vulnerabilities and the recognition of the need to protect data, information, and the means of processing them;

(2) *Policy level training* provides the ability to understand computer security principles so that executives can make informed policy decisions about their computer and information security programs;

(3) *Implementation level training* provides the ability to recognize and assess the threats and vulnerabilities to automated information resources so that the responsible managers can set security requirements which implement agency security policies; and

(4) *Performance level training* provides the employees with the skill to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

(b) Training audiences are groups of employees with similar training needs. Consistent with the Computer Security Training Guidelines, they are defined as follows:

(1) *Executives* are those senior managers who are responsible for setting agency computer security policy, assigning responsibility for implementing the policy, determining acceptable levels of risk, and providing the resources and support for the computer security program.

(2) *Program and Functional Managers* are those managers and supervisors who have a program or functional responsibility (not in the area of computer security) within the agency. They have primary responsibility for the security of their data. This means that they designate the sensitivity and criticality of data and processes, assess the risks to those data, and identify security requirements to the supporting data processing organization, physical facilities personnel, and users of their data. Functional managers are responsible for assuring the adequacy of all contingency plans relating to the safety and continuing availability of their data.

(3) *Information Resources Managers (IRM), Security, and Audit Personnel* are all involved with the daily management of the agency's information resources, including the accuracy, availability, and safety of these resources. Each agency assigns responsibility somewhat differently, but as a group these persons issue procedures, guidelines, and standards to implement the agency's policy for information security, and to monitor its effectiveness and efficiency. They provide technical assistance to users, functional managers, and to the data processing organization in such areas as risk assessment and available security products and technologies. They review and evaluate the functional and program groups' performance in information security.

(4) *Automated Data Processing (ADP) Management, Operations, and Programming Staff* are all involved with the daily management and operations of the automated data processing services. They provide for the protection of the data in their custody and identify to the data owners what those security measures are. This group includes such diverse positions as computer operators, schedulers, tape librarians, data base administrators, and systems and applications programmers. They provide the technical expertise for implementing security-related controls within the automated environment. They have primary responsibility for all aspects of contingency planning.

(5) *End Users* are any employees who have access to an agency computer system that processes sensitive information. This is the largest and most heterogenous group of employees. It consists of everyone from the executive who has a personal computer with sensitive information to data entry clerks.

(c) The training guidelines developed by the National Institute of Standards and Technology identify five subject areas. They are:

(1) *Computer security basics* is the introduction to the basic concepts behind computer security practices and the importance of the need to protect the information from vulnerabilities to known threats;

(2) *Security planning and management* is concerned with risk analysis, the determination of security requirements, security training, and internal agency organization to carry out the computer security function;

(3) *Computer security policies and procedures* looks at Governmentwide and agency-specific security practices in the areas of physical, personnel software, communications, data, and administrative security;

(4) *Contingency planning* covers the concepts of all aspects of contingency planning, including emergency response plans, backup plans and recovery plans. It identifies the roles and responsibilities of all the players involved; and

(5) *Systems life cycle management* discusses how security is addressed during each phase of a system's life cycle (e.g. system design, development, test and evaluation, implementation, and maintenance). It addresses procurement, certification, and accreditation.

(d) The statute defines the term *sensitive information* as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

§ 930.302 Training requirement.

The head of each agency shall identify employees responsible for the management or use of computer systems that process sensitive information and provide the following training (consult ''Computer Security Training Guidelines,'' NIST Special Publication 500–172[1], for more detailed information) to each of these groups:

(a) Executives shall receive awareness training in computer security basics, computer security policy and procedures, contingency planning, and systems life cycle management; and policy level training in security planning and management.

(b) Program and functional managers shall receive awareness training in computer security basics; implementation level training in security planning and management, and computer security policy and procedures; and performance level training in contingency planning and systems life cycle management.

(c) IRM, security, and audit personnel shall receive awareness training in computer security basics; and performance level training in security planning and management, computer security policies and procedures, contingency planning, and systems life cycle management.

(d) ADP management and operations personnel shall receive awareness training in computer security basics;

[1] Copies may be ordered from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402–9325.