

§930.211

equivalent, a list of acceptable geographical locations, and a copy of the reduction in force notice at any time after the receipt of the specific reduction in force notice, but not later than 90 days after the date of separation, furlough for more than 30 days, or demotion.

(ii) Eligibility on the OPM priority referral list expires 2 years after the effective date of the reduction in force action.

(iii) Referral and selection of administrative law judges are made without regard to selective certification or special qualification procedures.

(iv) Termination of eligibility on the OPM priority referral list takes place when an administrative law judge submits a written request to terminate eligibility, accepts a permanent full-time administrative law judge position, or declines one full-time employment offer as an administrative law judge at or above the level held when reached for reduction in force at geographic locations indicated as acceptable under paragraph (c)(2)(i) of this section.

(3) When there is no administrative law judge available on the agency's re-employment priority list, an agency may fill a vacant administrative law judge position only from OPM's priority referral list, unless the agency obtains prior approval from OPM to fill the vacant position through competitive examining, promotion, transfer, reassignment, or reinstatement procedures. OPM will grant such approvals only under extraordinary circumstances. The agency must demonstrate that the potential administrative law judge candidate possesses experience and qualifications superior to any available displaced administrative law judge on OPM's priority referral list.

§930.211 Actions against administrative law judges.

(a) *Procedures.* An agency may remove, suspend, reduce in level, reduce in pay, or furlough for 30 days or less an administrative law judge only for good cause established and determined by the Merit Systems Protection Board on the record and after opportunity for a hearing before the Board as pre-

5 CFR Ch. I (1-1-08 Edition)

scribed in 5 U.S.C. 7521 and 5 CFR part 1201. Procedures for adverse actions by agencies under part 752 of this chapter do not apply to actions against administrative law judges.

(b) *Status during removal proceedings.* In exceptional cases when there are circumstances in which the retention of an administrative law judge in his or her position, pending adjudication of the existence of good cause for his or her removal, is detrimental to the interests of the Federal Government, the agency may:

(1) Assign the administrative law judge to duties consistent with his or her normal duties in which these circumstances would not exist;

(2) Place the administrative law judge on leave with his or her consent;

(3) Carry the administrative law judge on annual leave, sick leave, leave without pay, or absence without leave, as appropriate, if he or she is voluntarily absent for reasons not originating with the agency; or

(4) If the alternatives in paragraphs (b)(1) through (b)(3) of this section are not available, the agency may consider placing the administrative law judge in a paid non-duty or administrative leave status.

(c) *Exceptions from procedures.* The procedures in paragraphs (a) and (b) of this section do not apply:

(1) In making dismissals or taking other actions under 5 CFR part 731;

(2) In making dismissals or other actions made by agencies in the interest of national security under 5 U.S.C. 7532;

(3) To reduction in force actions taken by agencies under 5 U.S.C. 3502; or

(4) In any action initiated by the Office of Special Counsel under 5 U.S.C. 1215.

Subpart C—Information Security Responsibilities for Employees who Manage or Use Federal Information Systems

AUTHORITY: 5 U.S.C. 4118; Pub. L. 107-347, 116 Stat. 2899.

SOURCE: 69 FR 32836, June 14, 2004, unless otherwise noted.

§ 930.301 Information systems security awareness training program.

Each Executive Agency must develop a plan for Federal information systems security awareness and training and

(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance available on the NIST Web site, *http://csrc.nist.gov/publications/nistpubs/*, as follows:

(1) All users of Federal information systems must be exposed to security awareness materials at least annually. Users of Federal information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to Federal information systems and applications.

(2) Executives must receive training in information security basics and policy level training in security planning and management.

(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.

(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.

(b) Provide the Federal information systems security awareness material/

exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.

(c) Provide information systems security refresher training for agency employees as frequently as determined necessary by the agency, based on the sensitivity of the information that the employees use or process.

(d) Provide training whenever there is a significant change in the agency information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

PART 950—SOLICITATION OF FEDERAL CIVILIAN AND UNIFORMED SERVICE PERSONNEL FOR CONTRIBUTIONS TO PRIVATE VOLUNTARY ORGANIZATIONS

Subpart A—General Provisions

Sec.	
950.101	Definitions.
950.102	Scope of the Combined Federal Campaign.
950.103	Establishing a local campaign.
950.104	Local Federal Coordinating Committee responsibilities.
950.105	Principal Combined Fund Organization (PCFO) responsibilities.
950.106	PCFO expense recovery.
950.107	Lack of a qualified PCFO.
950.108	Preventing coercive activity.
950.109	Avoidance of conflict of interest.
950.110	Prohibited discrimination.

Subpart B—Eligibility Provisions

950.201	National/international eligibility.
950.202	National/international eligibility requirements.
950.203	Public accountability standards.
950.204	Local eligibility.
950.205	Appeals.

Subpart C—Federations

950.301	National and international federations eligibility.
950.302	Responsibilities of national and international federations.
950.303	Local federations eligibility.
950.304	Responsibilities of local federations.

Subpart D—Campaign Information

950.401	Campaign and publicity information.
950.402	Pledge form.