Rules and Regulations

Federal Register
Vol. 69, No. 113
Monday, June 14, 2004

OFFICE OF PERSONNEL MANAGEMENT

5 CFR Part 930

RIN 3206–AJ84

Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems

AGENCY: Office of Personnel Management.

ACTION: Final rule.

SUMMARY: The Office of Personnel Management (OPM) is issuing final regulations concerning information technology security awareness and training for agency personnel including contractors and other users of information systems that support the operations and assets of the agency. This regulation makes the rule clearer for expert and novice readers. It facilitates timely access to changes in information systems security awareness training guidelines and supplementary information systems training and standards resources through the use of the National Institute for Standards and Technology (NIST) website.

DATES: *Effective Date:* June 14, 2004.

FOR FURTHER INFORMATION CONTACT: LaVeen Ponds by phone at 202–606–1394, by TTY at (202) 418–3134, by fax at (202) 606–2329, or e-mail at *lmponds@opm.gov.*

SUPPLEMENTARY INFORMATION: The Office of Personnel Management (OPM) issued proposed regulations at 68 FR 52528, on September 4, 2003, to revise the rules that govern the training of employees responsible for the management or use of Federal computer systems. We proposed streamlining the regulation where appropriate; removed text; and added a requirement for agencies to refer to the National Institute of Standards and Technology (NIST) website for the most current information on information systems security awareness and training guidelines. The 30-day comment period ended on October 6, 2003. We received comments from five Federal agencies.

One agency concurred with the proposed changes and stated that the changes are particularly beneficial.

Two agencies pointed out that the Federal Information Security Management Act (FISMA), title III of Public Law 107–347 (116 Stat 2948), and the E-Government Act of 2002, Public Law 107–347 (116 Stat 2899), repealed sections of the Computer Security Act of 1987, Public Law 100–235 (101 Stat 1724). We have changed the authority source accordingly.

One of these agencies noted that the language in the ''Regulatory Flexibility Act'' section of the proposed regulation did not include all individuals that the regulation will affect. We concur and have changed the language to reflect the individuals listed in Public Law 107–347 (116 Stat 2951) that are affected by this regulation.

One agency pointed out that Office of Management and Budget (OMB) Circular A–130, appendix III, also addressed OPM's responsibility to assure that its regulations concerning computer security training for Federal civilian employees are effective. Therefore, the agency suggested that OMB Circular A–130, appendix III, be referenced in the regulation. We believe the authority references are sufficient and establish the legal requirements for the regulation and that additional references are not necessary. Two agencies noted that the proposed regulation referenced a NIST website location that did not address the guidance for security awareness and training. A more direct link has been included in section 930.301(a). One of these agencies also suggested changing the word ''computer'' to ''information technology'' to better reflect the scope of the regulations and NIST guidance. We concur and have made the change where appropriate in the final regulation. Additionally, it is important to note the purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls over any information resources that support Federal operations and assets. To that end, FISMA defines information system security to mean protecting any Federal information and information systems, which includes information technology (IT) systems, from unauthorized access, use, disclosure, disruption, modification, or destruction.

This agency also recommended that 5 CFR 903.301(a)(1) require all IT users be exposed to security awareness materials ''regularly'' versus ''at least annually.'' We do not concur. A standard and specified timeframe for training best serves the intent of the law and encourages agencies to ensure IT users' continual IT security vigilance. We did not adopt this agency's suggestion to address professionalization or certification to ensure a level of knowledge or competence because it is beyond the scope of this regulation.

The same agency recommended adding a section requiring agencies to provide training commensurate with IT systems criticality and level of risk imposed by the untrained user. We did not adopt this recommendation because this issue is addressed in the Act and covered in 5 CFR § 903.301(b) through (d). We have incorporated the agency's suggestion to change NIST ''policy'' to NIST ''guidelines'' throughout the regulation. The agency comment that NIST guidance is based on roles and responsibilities and not position titles, as indicated in the regulation, does not require a change. The regulation requires role-specific training. Identification of employees performing these roles by position title is illustrative only and does not differ from the role-specific training basis of NIST guidance.

Another agency suggested that the requirement to provide IT awareness material/exposure training to all new employees ''within 60-days of their appointment'' be changed to ''prior to the employee's use of IT systems.'' We concur and have changed the text pursuant to OMB Circular A–130, appendix III, part A, subsection A.

Waiver of 30-day delay in effectiveness

Pursuant to 5 U.S.C. 553(d)(3), good cause exists to waive the delay in effective date and make these regulations effective in less than 30 days. The delay in the effective date is being waived because the program changes do not mandate substantive change but will provide users more timely access to the most current applicable definitions and guidelines for

information technology security awareness training.

E.O. 12866, Regulatory Review

This rule has been reviewed by the Office of Management and Budget in accordance with E.O. 12866.

Regulatory Flexibility Act

I certify that these regulations would not have a significant economic impact on a substantial number of small entities because they would apply only to Federal personnel including contractors and other users of information systems that support the operations and assets of the agency.

List of Subjects in 5 CFR part 930

Administrative practice and procedure; Computer technology; Government employees; Motor vehicles.

Office of Personnel Management.

Kay Coles James,

Director.

■ Accordingly, OPM revises 5 CFR part 930, subpart C, as follows:

PART 930—PROGRAMS FOR SPECIFIC POSITIONS AND EXAMINATIONS (MISCELLANEOUS)

■ 1. Subpart C is revised to read as follows:

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

§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.

[FR Doc. 04–13319 Filed 6–10–04; 8:45 am]

BILLING CODE 6325–38–P

NUCLEAR REGULATORY COMMISSION

10 CFR Part 2

RIN 3150–AH31

Licensing Proceeding for a High-Level Radioactive Waste Geologic Repository; Licensing Support Network, Submissions to the Electronic Docket

AGENCY: Nuclear Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Nuclear Regulatory Commission is amending its Rules of Practice applicable to the use of the Licensing Support Network (LSN) and the electronic hearing docket in the licensing proceeding on the disposal of high-level radioactive waste at a geologic repository. The amendments establish the basic requirements and standards for the submission of adjudicatory materials to the electronic hearing docket by parties to the high-level radioactive waste licensing proceeding. The amendments also address the issue of reducing the unnecessary loading of duplicate documents on individual participant LSN document collection servers (Web sites); the continuing obligation of LSN participants to update their documentary material after the initial certification; the Secretary of the Commission's determination that the DOE license application is electronically accessible; and the provisions on material that may be excluded from the LSN.

DATES: *Effective Date:* July 14, 2004.

FOR FURTHER INFORMATION CONTACT: Francis X. Cameron, U.S. Nuclear Regulatory Commission, Washington DC 20555–0001, telephone (301) 415–1642, e-mail *FXC@nrc.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

The Commission's regulations in 10 CFR Part 2, Subpart J, provide for, among other things, the use of an electronic information management system to provide documents related to the high-level radioactive waste (HLW) repository licensing proceeding. Originally promulgated on April 14, 1989 (54 FR 14944), the information management system required by Subpart J is to have the following functions:

(1) The Licensing Support Network (LSN) provides full text search and retrieval access to the relevant documents of all parties and potential parties to the HLW repository licensing proceeding beginning in the time period before the U.S. Department of Energy (DOE) license application for the repository is submitted;

(2) The NRC Electronic Information Exchange (EIE) provides for electronic submission of filings by the parties, as well as the orders and decisions of the Atomic Safety and Licensing Board Panel (ASLBP), during the proceeding; and

(3) The Electronic Hearing Docket (EHD) provides for the development and