U.S. Department of Energy
Washington D.C.

NOTICE

DOE N 411.1

Approved: 8-27-03
Expires: 8-27-04

SUBJECT: SAFETY SOFTWARE QUALITY ASSURANCE FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIES FOR NUCLEAR FACILITIES AND ACTIVITIES

1. OBJECTIVE. To assign roles and responsibilities for improving the quality of safety software.

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. DOE Elements. Except for exclusions in paragraph 3b, this Notice applies to all Department of Energy (DOE) elements, including National Nuclear Security Administration elements, that develop, use, assess, establish requirements for, or provide direction for safety software that is used to analyze or guide safety-related decisions or to design or develop safety-related controls for DOE nuclear facilities or activities. (See Attachment 1.)

   b. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, *Naval Nuclear Propulsion Program*, this Notice does not apply to the naval reactors program.

4. RESPONSIBILITIES.

   a. Assistant Secretary for Environment, Safety and Health.

      (1) Ensures execution of the *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1, Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities* (IP), including designating a responsible manager to facilitate completion of all IP deliverables and commitments.

      (2) Establishes a "corporate" (DOE-wide) quality assurance (QA) function within the Office of Environment, Safety and Health that is responsible and accountable for the identification and resolution of Departmental crosscutting safety software issues, including research and development activities.

      (3) Establishes a panel of subject matter experts (SMEs) for safety software. The SME Panel functions will include—

         (a) assisting in the execution of the IP;

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Environment, Safety and Health

(b) providing input to the Office of Environment, Safety and Health regarding practical experience with development and implementation of effective safety software QA (SQA) programs and processes;

(c) providing input to the Office of Environment, Safety and Health regarding the use of safety software;

(d) identifying and addressing major safety software issues having crosscutting impact on the DOE complex;

(e) serving as a forum for sharing lessons learned, ideas, and proven processes/programs with the DOE complex;

(f) assisting in establishing relationships and participating with outside organizations involved in safety SQA; and

(g) recommending additional safety software for the “toolbox codes.”

(4) Establishes, implements, and maintains a central registry for the long-term maintenance and control of a set of safety software (i.e., toolbox codes), and develops, issues, and maintains guidance on the use of toolbox codes. Adds safety software to the toolbox codes.

(5) Captures and communicates safety software lessons learned and identifies new technology, innovative techniques, and actions needed to ensure software quality.

(6) Shares program Secretarial Officer (PSO) safety software assessment schedules and results throughout the Department.

(7) Develops and issues criteria review and approach documents (CRADs) for use by PSOs and field elements[1] to identify, select, and assess the quality of safety software.

(8) Identifies and participates in Government and non-Government standards bodies relevant to safety software and consistent with the DOE Technical Standards Program.

(9) Develops, issues, and maintains directives for safety software.

[1] The term “field elements,” as used in this directive, includes operations offices, field offices, site offices, area offices, project offices, service centers, and federally staffed laboratories.

(10) Ensures that the DOE Functions, Responsibilities, and Authorities Manual and the Office of Environment, Safety and Health Functions, Responsibilities, and Authorities (FRA) document incorporate Federal responsibilities and authorities for safety software.

(11) Briefs the Defense Nuclear Facilities Safety Board on the IP status approximately every 4 months.

(12) Updates the Technical Qualifications Program position list to identify the Federal positions whose duties and responsibilities require them to meet the Functional Area Qualification Standard (FAQS) for safety software.

(a) Qualifies those personnel who have responsibility for safety software to the requirements of the FAQS for safety software.

(b) Updates qualifications of other personnel if their FAQSs are revised to include safety software competencies.

b. Chief Information Officer. Provides support to the Assistant Secretary of Environment, Safety and Health, as requested, in establishing safety software requirements.

c. Secretarial Officers.

(1) Update the Technical Qualifications Program position list to identify the Federal positions whose duties and responsibilities require them to meet the FAQS for safety software.

(a) Qualify those personnel who have responsibility for safety software to the requirements of the FAQS for safety software.

(b) Update qualifications of other personnel if their FAQSs are revised to include safety software competencies.

(2) Ensure safety software assessments are scheduled and conducted in coordination with field element managers,[2] using approved CRADs. Provide assessment schedules and results to the Assistant Secretary for Environment, Safety, and Health.

(3) Support the development, review, and approval of safety software directives by the Office of Environment, Safety and Health.

[2] The term "field element managers," as used in this directive, includes operations office, site office, area office, project office, and service center managers and managers of federally staffed laboratories.

(4) Identify and implement applicable safety software standards, including DOE directives, consistent with quality assurance requirements in DOE O 414.1A, *Quality Assurance,* dated 9-29-99, or 10 CFR 830, Nuclear Safety Management, (whichever is applicable) and DOE G 200.1-1, *Software Engineering Methodology,* dated 5-21-97 (as appropriately graded).

(5) Identify and assign persons qualified to serve on the SME Panel for safety software.

(6) Support the Assistant Secretary of Environment, Safety, and Health, as requested and agreed upon, to meet IP commitments.

(7) Revise the PSO FRA documents to include Federal functions, responsibilities, and authorities for safety software.

d. Field Element Managers.

(1) Update the Technical Qualifications Program position list to identify the Federal positions whose duties and responsibilities require them to meet the Functional Area Qualification Standard (FAQS) for safety software.

(a) Qualify personnel who have responsibility for safety software to the requirements of the FAQS for safety software.

(b) Update qualifications of other personnel if their FAQSs are revised to include safety software competencies.

(2) Conduct assessments according to the established schedule for safety software using approved CRADs, and report the results to the cognizant PSOs.

(3) Use the unreviewed safety question process to address assessment results that question the validity of the software previously used to support the safety analysis and design process. (See 10 CFR 830.203, Unreviewed Safety Question Process, and DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements,* dated 10-24-01.)

(4) Revise the field element FRA document to include Federal functions, responsibilities, and authorities for safety software.

(5) Ensure that DOE-approved contractor QA programs are applied to safety software, in accordance with applicable laws, regulations, DOE directives, and adopted industry standards.

e. Office of Independent Oversight. Assesses the performance of DOE in implementing safety software requirements.

5. DEFINITIONS. The following definitions are taken from the IP. References in brackets following definitions indicate the original source when not the IP.

a. Central Registry. An organization designated to be responsible for the storage, control, and long-term maintenance of the Department's safety analysis "toolbox codes." The central registry may also perform this function for other codes if the Department determines that this is appropriate.

b. Firmware. The combination of a hardware device and computer instructions and data that reside as read-only software on that device. [IEEE Standard 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*]

c. Nuclear Facility. A reactor or a nonreactor nuclear facility where an activity is conducted for or on behalf of DOE and includes any related area, structure, facility, or activity to the extent necessary to ensure proper implementation of the requirements established by 10 CFR 830. [10 CFR 830]

d. Safety Analysis and Design Software. Computer software that is not part of a structure, system, or component (SSC) but is used in the safety classification, design, and analysis of nuclear facilities to ensure—

- the proper accident analysis of nuclear facilities;
- the proper analysis and design of safety SSCs; and
- the proper identification, maintenance, and operation of safety SSCs;

e. Safety-Class Structures, Systems, and Components (SC SSCs). SSCs, including portions of process systems, whose preventive and mitigative function is necessary to limit radioactive hazardous material exposure to the public, as determined from the safety analyses. [10 CFR 830]

f. Safety-Significant Structures, Systems, and Components (SS SSCs). SSCs which are not designated as safety-class SSCs, but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from safety analyses. [10 CFR 830]

As a general rule of thumb, SS SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in prompt worker fatalities, serious injuries, or significant radiological or chemical exposure to workers. The term serious injuries, as used in this definition, refers to medical treatment for immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb).

The general rule of thumb cited above is neither an evaluation guideline nor a quantitative criterion. It represents a lower threshold of concern for which an SS SSC designation may be warranted. Estimates of worker consequences for the purpose of SS SSC designation are not intended to require detailed analytical modeling. Consideration should be based on engineering judgment of possible effects and the potential added value of SS SSC designation. [DOE G 420.1-1]

g. Safety Software. Includes both safety system software and safety analysis and design software.

h. Safety Structures, Systems, and Components (SSCs). The set of safety-class SSCs and safety-significant SSCs for a given facility. [10 CFR 830]

i. Safety System Software. Computer software and firmware that performs a safety system function as part of a structure, system, or component (SSC) that has been functionally classified as Safety Class (SC) or Safety Significant (SS). This also includes computer software such as human-machine interface software, network interface software, programmable logic controller (PLC) programming language software, and safety management databases that are not part of an SSC but whose operation or malfunction can directly affect SS and SC SSC functions.

j. Software. Computer programs, operating systems, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. [IEEE Standard 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*]

k. Toolbox Codes. A small number of standard computer models (codes) supporting DOE safety analysis, having widespread use, and of appropriate qualification that are maintained, managed, and distributed by a central source. These codes are verified and validated and constitute a "safe harbor" methodology. That is to say, the analysts using these codes do not need to present additional defense as to their qualification, provided that they are sufficiently qualified to use the codes and the input parameters are valid. It may also include commercial or proprietary design codes where DOE considers additional SQA controls are appropriate for repetitive use in safety applications and there is a benefit to maintain centralized control of the codes.

6. REFERENCES.

a. U.S. Department of Energy. *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1, Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities,* issued by Memorandum from Secretary Spencer Abraham to the Honorable John T. Conway, Chairman, DNFSB, March 13, 2003.

b. Executive Order 12344, *Naval Nuclear Propulsion Program*.

c. 10 CFR 830, Nuclear Safety Management.

d. DOE G 200.1-1, *Software Engineering Methodology* dated 5-21-97.

e. DOE M 411.1-1B, *Safety Management Functions, Responsibilities, and Authorities,* dated 5-22-01.

f. DOE O 414.1A, *Quality Assurance,* dated 9-29-99.

g. DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements,* dated 10-24-01.

7. CONTACT. For additional information or assistance in interpreting or implementing this Notice, please contact Chip Lagdon 301-903-4218 or Chip.Lagdon@eh.doe.gov.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

DOE ORGANIZATIONS TO WHICH DOE N 411.1 IS APPLICABLE

This Notice is applicable to the following DOE organizations and their associated Federal field elements.

Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Environment, Safety and Health
Office of Environmental Management
Office of Independent Oversight and Performance Assurance
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Science
Office of Security

DOE ORGANIZATIONS TO WHICH DOE N 411.1 IS NOT APPLICABLE

Office of the Secretary
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
Office of Policy and International Affairs
Office of Public Affairs
Secretary of Energy Advisory Board
Office of Worker and Community Transition
Office of Electric Transmission and Distribution
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power AdministrationWestern Power Administration