The Secretary of Energy
Washington, DC 20585

March 13, 2003

The Honorable John T. Conway
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW
Suite 700
Washington, D.C. 20004-2901

Dear Mr. Chairman:

Enclosed is the Department of Energy's Implementation Plan for the Defense Nuclear Facilities Safety Board's Recommendation 2002-1, *Quality Assurance for Safety Related Software*. The Department considers its efforts to improve software quality assurance as a key element in our ongoing initiatives to improve quality management systems at defense nuclear facilities. We will keep you and your staff informed of our progress in meeting the commitments in this Plan.

Ms. Beverly Cook, Assistant Secretary for Environment, Safety and Health, is the Department of Energy executive responsible for our Quality Assurance Program. She is also responsible for ensuring the successful completion of this Implementation Plan. If you have any questions, please call Ms. Cook at (202) 586-6151.

Sincerely,

Spencer Abraham

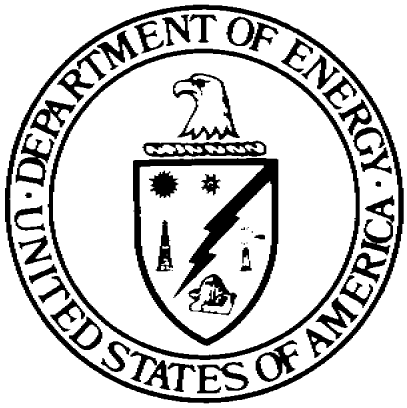
Enclosures

cc:
J. McMonigle, S
M. Whitaker, S-31.

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



Washington, D.C. 20585

March 13, 2003

Executive Summary

The Defense Nuclear Facilities Safety Board (Board) issued Recommendation 2002-1, *Quality Assurance for Safety-Related Software*, on September 23, 2002. In that Recommendation, the Board noted its concerns regarding the quality of the software used to analyze and guide safety-related decisions, the quality of the software used to design or develop safety-related controls, and the proficiency of personnel using the software. In addition, the Board noted that software performing safety-related functions in distributed control systems, supervisory control and data acquisition systems (SCADAs), and programmable logic controllers (PLCs) requires appropriate quality assurance controls to provide adequate protection for the public, the workers, and the environment.

The Department of Energy (DOE or Department) accepted the Board's Recommendation on November 21, 2002. The Department analyzed the Board's Recommendation in light of an earlier evaluation of the impact of potential software problems on safety systems that protect the public, workers, and the environment. The Department agrees that potential weaknesses in this software could have an effect on these safety systems. Although the Department had undertaken an initiative to develop a Quality Assurance Improvement Plan that would have addressed some of the issues identified by the Board, the Department agrees with the Board's observation that these initiatives had not yet produced any substantial results. The Department committed to developing an Implementation Plan in the Secretary's acceptance letter of November 21, 2002.

This Implementation Plan defines the actions and processes that will be taken to ensure the quality of safety software at defense nuclear facilities. Safety software includes both safety system software and safety analysis and design software as defined in this Implementation Plan. Actions taken in this Plan will build on existing initiatives as appropriate. They include:

- The identification, documentation and communication of roles, responsibilities and authorities for software quality assurance (SQA). These will initially be documented and communicated in a DOE Notice and eventually will be included in updated DOE directives, the Functions, Responsibilities and Authorities Manual, and related documents.

- The identification of Federal personnel in both Headquarters and the Field that have responsibility related to safety software. These personnel will be required to satisfy the competency requirements identified in a Technical Qualification Standard.

- An assessment of safety system software to determine its current status and an assessment of the effectiveness of SQA programs for safety analysis and safety design software. Corrective actions will be identified and completed as appropriate. If any of the assessments described in this plan identify a problem with existing software, the problem will be resolved using the Unreviewed Safety Question (USQ) process. Generic USQs will be used to the extent possible rather than multiple facilities developing separate Unreviewed Safety Question Determinations (USQD) for the same problem.

- Identification of a set of safety analysis "toolbox" codes that are commonly used across the Department, the upgrade of those codes to a prescribed qualification, and the establishment of a Central Registry to facilitate maintenance, technical support, configuration management, training, and notification to users of problems and revisions to these codes. The toolbox could include proprietary or commercial design codes where DOE considers additional SQA controls are appropriate for repetitive use and there is a benefit to centralized control of the codes.

- The identification and development of requirements and guidance for safety SQA based on existing industry or Federal agency standards. These requirements and guidance will be of sufficient rigor to ensure the reliability of safety software at defense nuclear facilities based on risk and complexity.

- A continuous improvement process that includes the identification of SQA experts across the Department who will provide input to management regarding SQA programs. This process will also provide an interface with outside organizations and agencies to facilitate the sharing of lessons learned and new technology.

Overall execution of this Implementation Plan is the responsibility of the Assistant Secretary for Environment, Safety and Health. A Responsible Manager will be assigned to ensure individuals responsible for deliverables and commitments identified within this Implementation Plan complete their actions. However, responsibility for implementing software quality assurance rests with the line managers and they are responsible for many of the deliverables associated with commitments made within this Implementation Plan. This includes ensuring that the necessary resources are provided.

Table 1 provides a summary of commitments made in this Implementation Plan, which are described further in Section 4.

TABLE OF CONTENTS

LIST OF TABLES

APPENDICES

1.0 BACKGROUND

The Defense Nuclear Facilities Safety Board (Board or DNFSB) issued Recommendation 2002-1 on September 23, 2002 (Appendix C). The Department of Energy (DOE or Department) accepted the Board's Recommendation on November 21, 2002 (Appendix D). Prior to the Board's issuing this Recommendation, DNFSB Technical Report 25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities,* was issued in January 2000, and three public meetings were conducted on the subject of quality assurance (QA) – including software quality assurance (SQA). Subsequently, the Department developed a Quality Assurance Improvement Plan that would have addressed some of the issues identified by the Board. However, the Department agrees with the Board's observation that this effort had not yet produced substantial results.

The Board stated in Recommendation 2002-1 that the robustness and reliability of many structures, systems, and components (SSCs) throughout DOE's defense nuclear complex depend on the quality of the software used to analyze and guide these decisions, the quality of the software used to design or develop controls, and proficiency in use of the software. In addition, software that performs safety-related functions in distributed control systems, supervisory control and data acquisition systems (SCADAs), and programmable logic controllers (PLCs) require the same high quality needed to provide adequate protection for the public, the workers, and the environment. Other types of software, such as databases used in safety management activities, can also serve important safety functions and deserve a degree of quality assurance commensurate with their contribution to safety.

The Board recommended that the Department define specific responsibilities and authorities for safety SQA, and to assign those responsibilities and authorities to individuals with the necessary technical expertise. The Board also recommended that design and analysis software be identified and controlled, that the Department establish specific directives in the area of SQA and that a continuous improvement process be implemented to maintain and upgrade software as necessary.

The Department completed its own analysis of the Board's Recommendation and evaluated the impact of potential safety software problems on safety systems that protect the public, workers, and the environment. The Department agrees that potential weaknesses in this type of software could negatively impact these safety systems. The Department committed to developing an Implementation Plan as described in the Secretary's acceptance letter of November 21, 2002, that will result in the following:

- Clear assignment of organizational roles, responsibilities and authorities for safety software.
- Establishment of the infrastructure necessary to ensure an effective software quality assurance program, including personnel with the appropriate skill and expertise.
- Implementation of processes to identify safety analysis and design codes and ensure that they are subject to verification and validation appropriate for the application.

- Establishment of requirements and guidance for a rigorous software quality assurance process, which will include the use of industry or Federal agency standards where practical.
- A process that will track continuous improvements and initiatives in software technology. This information will be used as a basis for maintaining safety software and will be shared across the complex.

The response team for this Recommendation reviewed and studied the SQA initiatives that are currently underway within various organizations across the Department. Actions identified in this Implementation Plan (IP) build upon these initiatives as appropriate.

2.0 UNDERLYING CAUSES

There have been several initiatives across the Department to improve SQA. However, there is not an integrated infrastructure that includes sufficient directives to ensure the implementation of a rigorous and consistent SQA process across the Department. Roles, responsibilities, and authorities are not always clearly defined or consistently assigned. There is no consensus set of training requirements for SQA and there has been insufficient oversight of SQA activities.

The Department recognizes the need to establish a rigorous and effective SQA program. In evaluating Recommendation 2002-1, previous correspondence from the Board's public meetings and Technical Report 25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*, the Department concluded that an integrated and effective SQA infrastructure does not exist throughout DOE's defense nuclear complex.

3.0 BASELINE ASSUMPTIONS

The Department made the following baseline assumptions in developing its Recommendation 2002-1 Implementation Plan:

- IP execution is based on target-level funding approved by Congress in an atmosphere of stable mission requirements. New SQA requirements identified as a result of this IP will be applied to software currently in use, as well as to new software. If any of the assessments described in this plan identify a problem with existing software, the problem will be resolved using the Unreviewed Safety Question (USQ) process. Generic USQs will be used to the extent possible to preclude the need for multiple facilities to perform separate Unreviewed Safety Question Determinations (USQDs) for the same problem.

- Actions identified in this IP are those necessary to address potential safety issues. The Department may take additional actions outside of this IP to address non-safety issues.

- There are sufficient industry or Federal agency standards available to address DOE software quality assurance needs.

4.0 SAFETY ISSUE RESOLUTION

The scope of this IP includes safety software at the Department's defense nuclear facilities. *Safety software*, as defined by this IP, includes both safety system software and safety analysis and design software. *Safety system software* is computer software and firmware that performs a safety system function as part of a 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, 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 function. *Safety analysis and design software* is software that is not part of an SSC but is used in the safety classification, design and analysis of nuclear facilities to ensure proper: accident analysis of nuclear facilities; analysis and design of safety SSCs; and identification, maintenance, and operation of safety SSCs.

The types of safety software that will be considered when determining the applicability of this IP include:

- Custom software developed by or for the Department;
- Commercial off-the-shelf software;
- Instrumentation and control software, such as SCADAs and PLCs – including embedded software and firmware;
- Calculation software, such as spreadsheets and math programs (along with their associated user files) used to perform safety analysis and design calculations; and
- Database programs and associated user files used to maintain control of information that has nuclear safety implications.

Each commitment within this IP is supported by an Issue Description describing the background, the Board's Recommendation, the Resolution Approach to address the Board's Recommendation, and the Deliverables/Milestones to address the commitment. Actions will be taken to ensure the quality and integrity of safety software at defense nuclear facilities. The following sections describe the actions that will be taken.

<u>Roles and Responsibilities</u>

- Identify, document, and communicate roles, responsibilities, and authorities for all aspects of SQA. This will initially be documented and communicated in a DOE Notice, and will eventually be included in updated directives, the Functions, Responsibilities, and Authorities Manual, and related documents.

- Identify Federal personnel in both Headquarters and Field Elements that have responsibility related to safety software. These personnel will be required to satisfy the competency requirements identified in a Technical Qualification Standard.

Computer Codes

- Assess safety system software to determine its current status and assess the effectiveness of SQA programs for safety analysis and safety design software. Corrective actions will be identified and completed as appropriate.

- Identify safety analysis "toolbox" codes that are commonly used across the Department, upgrade the codes to a prescribed qualification, and establish a Central Registry to facilitate maintenance, technical support, configuration management, training, and notification to users of problems and revisions to these codes.

Requirements and Guidance

- Identify and develop requirements and guidance for safety software quality assurance based on existing industry or Federal agency standards. These requirements and guidance will be sufficiently rigorous to ensure the reliability of safety software at defense nuclear facilities based on risk and complexity.

Continuous Improvement

- Implement a continuous improvement process that includes the formation of an Office of Quality Assurance and the identification of SQA experts across the Department to provide support to that Office and assistance in implementing this IP. This process will also provide for interfacing with outside organizations and agencies to enable an exchange of lessons learned and new technology.

4.1 Roles and Responsibilities

Issue Description

The Department has been slow in responding to issues relating to SQA. One of the causes for this is the lack of clearly defined roles, responsibilities, and authorities for safety software. Although QA roles and responsibilities are defined within the Department, SQA is not specifically addressed. Additionally, qualification requirements for DOE personnel whose duties involve quality assurance for safety software at defense nuclear facilities are neither clearly defined nor verified.

Board Recommendation

Define responsibility and authority for the following: developing SQA guidance, conducting oversight of the development and use of software important to safety, and directing research and development. Roles and responsibilities should address all software important to safety, including, at a minimum, design software, instrumentation and control software, software for

analysis of consequences of potential accidents, and other types of software, such as databases used for safety management functions.

Assign those responsibilities and authorities to offices/individuals with the necessary technical expertise.

Resolution Approach

The Clinger-Cohen Act assigns the authority and responsibility for software policy and oversight to the Chief Information Officer (CIO). The Assistant Secretary for Environment, Safety, and Health (EH) has lead responsibility for safety policy, direction, and guidance. There is a convergence of these responsibilities in the area of safety software. The office of the CIO has more expertise in SQA in general, but software safety is a specialized sub-discipline that requires both safety assurance expertise and SQA expertise. As such, EH will have the lead responsibility for promulgating requirements and guidance through the directives system for safety software after formal coordination with the CIO.

The Department will review the current assignment of roles and responsibilities as well as the technical qualification requirements for personnel serving in positions whose duties relate to SQA. The actions and commitments in this IP will lead to well-defined roles, authorities, and responsibilities for implementing an effective SQA program. Consistent with the principles of Integrated Safety Management, organizations and individuals assigned SQA responsibilities will be required to possess technical capabilities commensurate with their duties. Responsibility and authority for activities such as developing SQA guidance, conducting oversight of the development and use of safety software, and directing research and development will be defined. Roles and responsibilities will be identified for safety software used for design, instrumentation and control (I&C), consequence analysis, and other types of software, such as databases used for safety management functions. It is envisioned that this will include responsibilities for the CIO, EH, Program Offices, Field Elements, and contractors.

The Department will issue a DOE Notice that specifies SQA roles, responsibilities, and authorities by organizational element. After all of the directives associated with SQA have been approved and issued (see Section 4.3) DOE M 411.1, *Safety Management Functions, Responsibilities, and Authorities Manual* (FRAM) and related Headquarters and field Functions, Responsibilities, and Authorities (FRA) documents will be updated, approved, and issued. When the FRAM and FRAs have been issued, the DOE Notice will be cancelled.

To ensure that Federal personnel with significant SQA responsibilities have the necessary technical capabilities to carry out their duties, technical qualification requirements will be specified in the appropriate Technical Qualification Standards. This process will be coordinated with the Federal Technical Capability Panel (FTCP) in accordance with the requirements of the DOE M 426.1, *Federal Technical Capability Manual*.

Deliverables/Milestones

Commitment 4.1.1: Issue a DOE Notice that identifies, documents, and communicates roles, responsibilities, and authorities for SQA by organizational element.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: DOE Notice

Due Date: July 2003

Commitment 4.1.2: Establish technical qualification requirements for Federal personnel whose duties and responsibilities require them to provide assistance, guidance, direction, oversight, or evaluation of safety software QA activities.

Lead Responsibility: Chair, Federal Technical Capability Panel (FTCP)

Deliverable: Software Engineer Technical Qualification Standard (or revision of an existing Qualification Standard)

Due Date: November 2003

Commitment 4.1.3: Identify the Federal positions whose duties and responsibilities require them to provide assistance, guidance, direction, oversight, or evaluation of safety software QA activities.

Lead Responsibility: Program Secretarial Officers (PSOs) and Field Element Managers

Deliverable: Technical Qualification Program (TQP) position list updated to include SQA positions

Due Date: October 2003

Commitment 4.1.4: Personnel assigned to SQA positions achieve qualification per the requirements of the Technical Qualification Program.

Lead Responsibility: PSOs and Field Element Managers

Deliverable: FTCP TQP Status Report that includes the identification of at least one qualified SQA position for each organization that requires qualified personnel.

Due Date: September 2004

Commitment 4.1.5: Revise the FRAM to incorporate Federal responsibilities and authorities for SQA.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Approved FRAM Revision

Due Date: December 2003

Commitment 4.1.6: Revise the Headquarters and Field Element FRA documents to incorporate Federal responsibilities and authorities for SQA.

Lead Responsibility: PSOs and Field Element Managers

Deliverable: Approved FRA Revisions

Due Date: April 2004

4.2 Computer Codes

Issue Description

Safety controls and their functional classifications are often based on software used to evaluate the consequences of potential accidents. The robustness and reliability of many SSCs throughout DOE's defense nuclear complex can be affected by the quality of the software used to support safety analysis, the quality of the software used to design or develop controls, and proficiency in use of the software. In addition, software that performs safety functions in distributed control systems, SCADAs, and PLCs require appropriate SQA controls in order to provide adequate protection for the public, workers, and the environment. Without an integrated and effective SQA infrastructure, there is the potential for both errors in technical output from software used in safety analyses and design, and incorrect performance of instrumentation and controls for safety systems.

Board Recommendation

Identify software that would be recommended for use in performing design and analyses of SSCs important to safety, and for analysis of expected consequences of potential accidents.

Identify an organization responsible for management of each of these software tools, including SQA, technical support, configuration management, training, notification to users of problems and fixes, and other official stewardship functions.

Resolution Approach

The Department will upgrade selected codes recognized to be high-use, or which could have significant consequences in the event of failure. The Department will establish a set of computer codes that will be under configuration control and managed by a single organization. These codes will be established as part of a "toolbox." These toolbox codes are, in principle, a small number of standard computer codes having widespread application and appropriate qualification that are managed and distributed for implementation by a central source know as the "Central Registry." Generally, codes in the toolbox will have been developed and maintained within the DOE complex. However, it may also include commercial or proprietary design codes where DOE considers additional SQA controls are appropriate for repetitive use of the codes in safety applications, and there is a benefit to centralized control of the codes.

The Central Registry organization will coordinate the use of the toolbox codes and assist users in configuration control, distribution, and serve as a point of contact for resolving user issues. The code owner will be responsible for ensuring that the code is maintained in accordance with established SQA requirements. The Central Registry will work closely with the code owner to ensure that adequate technical support and training are available. While a location has not been identified, an existing software center or one of the national laboratories are probably good candidates to support these functions using existing infrastructure.

The Department expects that some remedial effort will be required for most of the toolbox codes. As SQA issues with each code are resolved, they will be placed under configuration control and identified in the registry. Once the toolbox codes have been upgraded, they may be thought of as "safe harbor" tools in the context of 10 CFR 830, *Nuclear Safety Management*, and can be applied as necessary to support safety basis documentation. In most situations, the user would need to reference the toolbox code and version, and demonstrate that the code is being applied in the proper context using appropriate inputs.

Safety system software used in support of nuclear facility processes can directly or indirectly affect the performance of intended safety functions. The types of systems associated with safety system software vary greatly in nature, design, and age. They are not amenable to the generic categorization used for accident analysis codes. To deal with these uncertainties, the Department will conduct an assessment of safety system software. This will allow for both the identification of the safety system computer software and firmware and the assessment of its operability. To ensure that this is accomplished in a consistent manner, criteria and guidance for identifying the software, selecting the software to be assessed, and conducting the assessments will be developed. Headquarters and field organizations will review the criteria and guidance and submit a schedule for completing their assessments. The results of the assessments will be documented in a report along with the identification of any required corrective actions to ensure the readiness of the software. Those systems that have received DNFSB Recommendation 2000-2 IP reviews, using the associated Criteria and Review Approach Document (CRAD) that included SQA, may be able to use those reviews as a basis for these assessments.

To provide interim justification for operation under the current system (i.e., prior to the approval and implementation of new SQA requirements and guidance), an assessment of current safety analysis and design software will also be conducted. These reviews will also be conducted using approved criteria and guidance, and will result in the development of an assessment report and the identification of any corrective actions required to ensure the validity of the software. The reviews will also ensure that design organizations have an SQA process for SSC design and performance analysis software that includes functional classification of the software, verification of applicability of the software, configuration management, and error reporting and resolution as a minimum. These reviews will only be conducted on software that is currently in use, not on software that may have been previously used as part of a safety analysis and design process. Should an issue arise that questions the validity of software previously used to support design or development, it will be resolved using the USQ process. Generic USQs will be used to the extent possible rather than multiple facilities developing separate USQDs for the same problem.

Deliverables/Milestones

Commitment 4.2.1: Identify the safety analysis codes that will be included as part of the Department's "toolbox" codes.

4.2.1.1 Identify the codes used for safety analysis to be part of the Safety Analysis Code Toolbox.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: List identifying the toolbox codes

Due Date: Complete

4.2.1.2 Establish SQA criteria for the safety analysis "toolbox" codes.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: SQA plan (including criteria) for toolbox codes

Due Date: July 2003

4.2.1.3 Perform a gap analysis of the "toolbox" codes to determine the actions needed to bring the code into compliance with the SQA qualification criteria, and develop a schedule with milestones to upgrade each code based on the gap analysis results.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Schedule with milestones to upgrade each code based on the gap analysis results

Due Date: November 2003

4.2.1.4 Issue code-specific guidance reports on use of the "toolbox" codes identifying applicable regimes in accident analysis, default inputs, and special conditions for use.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Code-specific guidance reports provided to the Central Registry

Due Date: September 2003

4.2.1.5 Conduct a survey of design codes currently in use to determine if any should be included as part of the toolbox codes.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Report on results of design code review

Due Date: December 2003

Commitment 4.2.2: Establish and implement a Central Registry for the long-term maintenance and control of the safety analysis "toolbox" codes.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Memorandum from Deputy Secretary of Energy establishing a Central Registry

Due Date: August 2003

Commitment 4.2.3: Identify safety system software (computer software and firmware) used in instrumentation or process control processes for nuclear facilities; assess its adequacy and implement corrective actions as necessary.

4.2.3.1 Develop criteria and guidance for the identification, selection, and assessment of safety system software and firmware at defense nuclear facilities.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Criteria review and approach document (CRAD)

Due Date: August 2003

4.2.3.2 Establish a schedule to complete the identification, selection, and assessment of safety system software and firmware at defense nuclear facilities.

Lead Responsibility: PSOs and Field Element Managers

Deliverable: Schedule of assessments

Due Date: October 2003

4.2.3.3 Complete the identification, selection, and assessment of safety system software and firmware at defense nuclear facilities.

Lead Responsibility: Field Element Managers

Deliverable: Reports to the PSO detailing the results of the assessments, any concerns with the quality of existing safety system software, and the actions necessary to address the concerns

Due Date: In accordance with the schedules established in 4.2.3.2

Commitment 4.2.4: Assess the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate and implement corrective actions as necessary.

4.2.4.1 Develop criteria and guidance to assess the processes that are in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Criteria Review and Approach Document (CRAD)

Due Date: August 2003

4.2.4.2 Establish a schedule to complete the assessment of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.

Lead Responsibility: PSOs and Field Element Managers

Deliverable: Schedule of assessments

Due Date: October 2003

4.2.4.3 Complete the assessments of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.

Lead Responsibility:	Field Element Managers
Deliverable:	Reports to the PSO indicating the results of the assessments, any concerns with the quality of existing codes, and the actions necessary to address the concerns.
Due Date:	In accordance with the schedules established in 4.2.4.2

4.3 Requirements and Guidance

Issue Description

Although there are many adequate industry or Federal agency standards for SQA, DOE has not established requirements or guidance that clearly defines those standards necessary for safety applications. Absent such guidance, some computer codes are not always reviewed for the level of quality expected for operations at defense nuclear facilities. A lack of clear direction on appropriate standards and requirements for quality assurance of safety software and its use leads to the potential for incorrectly or inadequately analyzing hazards. In addition, software-controlled systems with a safety function may not perform as intended.

Board Recommendation

Establish requirements and guidance in the DOE directives system for a rigorous SQA process, including specific guidance on the following: grading of requirements according to safety significance and complexity; performance of safety reviews, including failure analysis and fault tolerance; performance of verification and validation testing; and training to ensure proficiency of users.

Resolution Approach

The Department will conduct a review to identify industry or Federal agency standards that are appropriate for the Department and its contractors. Some DOE sites have made significant progress in establishing SQA programs, and the U.S. Nuclear Regulatory Commission (NRC) has developed expectations regarding how their licensees are to tailor and apply industry or Federal agency standards. The Department will draw on the experience of DOE sites, the NRC, and nuclear utilities in determining the standards that best serve its needs.

It is assumed that there are sufficient industry or Federal agency standards that address the Department's SQA needs. In addressing the Board's Recommendation, the Department will make improvements in the directives system to better describe when and how organizations apply these existing standards to SQA. This will be accomplished through new or revised DOE Policies, Orders, Manuals, Standards, or Guides. At a minimum, the new or revised directives will address:

- Grading SQA requirements based on risk, safety, facility lifecycle, complexity, and project quality requirements;
- Performing safety reviews of software configuration items that will address considerations such as failure analysis and fault tolerance;
- Developing procurement controls for acquisition of computer software and hardware that are provided with vendor-developed software and/or firmware;
- Applying SQA requirements to software lifecycles;
- Documenting and tracking customer requirements;
- Managing software configuration throughout the lifecycle;
- Performing verification and validation testing; and
- Training of personnel who use software in safety applications.

As part of the Department's normal business processes, subject matter experts (SMEs) at each site and applicable Headquarters organization will review the requirements and processes resulting from the revised/new directives. Each organization/site will determine the path necessary to address deficiencies and reduce risk to an acceptable level. Attributes such as short lifecycle and the generally low-hazard nature of the deactivation and decommissioning of facilities should be considered when making this determination. Contractual changes necessary to implement the directives will be accomplished and follow-up verifications will be conducted to ensure that implementation is effective. Actions identified in these verification reviews will be documented in an SQA directive implementation plan and schedule.

Deliverables/Milestones

Commitment 4.3.1: Conduct a review to identify the industry or Federal agency standards that are appropriate for DOE safety software.

Lead Responsibility:	Assistant Secretary for Environment, Safety and Health
Deliverable:	Report identifying appropriate industry or Federal agency standards.
Due date:	September 2003

Commitment 4.3.2: Issue new/revised directives (DOE Policies, Orders, Manuals, Standards, or Guides) required to invoke industry or Federal agency standards for safety software quality assurance.

4.3.2.1 Establish a schedule to develop, revise, approve, and issue required SQA directives.

Lead Responsibility:	Assistant Secretary for Environment, Safety and Health

Deliverable: Schedule to develop, revise, approve, and issue required SQA directives.

Due Date: October 2003

4.3.2.2 Issue required SQA directives.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Approved directives in accordance with the schedule issued in 4.3.2.1

Due Date: In accordance with the schedule established in 4.3.2.1

Commitment 4.3.3: Headquarters and Field Elements review the approved SQA directives and determine the actions necessary to implement the requirements.

Lead Responsibility: PSOs and Field Element Managers

Deliverable: SQA directive implementation plan and schedule

Due Date: Three months following issuance of SQA directives

4.4 Continuous Improvement

Issue Description

In addition to establishing the infrastructure for an integrated and effective SQA program, it is prudent that the Department ensure that these programs and processes are maintained and keep pace with evolving industry practices. This involves establishing an internal communications network within the Department and a network outside of the Department. Although these networks are functioning at various levels in some organizations, they are not integrated and therefore not always effective in ensuring a consistent application across the Department. Additionally, there is no consolidated and coordinated "body of knowledge" within the Department to keep pace with industry practices or to provide input to management regarding program changes to ensure software quality.

Board Recommendation

Identify evolving areas in software development in which additional research and development is needed to ensure software quality.

Resolution Approach

To ensure continuous improvement in the area of SQA, several elements are required. The Department must ensure that it stays current with industry and Federal agency standards and practices related to SQA. To accomplish this, a more formalized and coordinated effort will be taken to interface with other agencies, industries, and organizations with expertise in SQA. It should be noted that various organizations across the Department are undertaking significant SQA efforts, but these efforts are not always coordinated or shared. Although there is a longstanding group within the weapons community working together in the area of SQA, it has not had the support and involvement by all organizations in the defense nuclear complex.

To provide additional corporate leadership in the area of quality assurance (including SQA), EH will establish an "Office of Quality Assurance." This Office will serve as the Department's corporate focal point for quality assurance programs, processes, and procedures. The Office will identify and resolve Departmental crosscutting QA and SQA issues, and will support line management in their implementation of policy and requirements for the design, procurement, fabrication, construction, and operation of facilities across the Department.

Since there are a number of widely scattered activities related to safety software, it is desirable to establish a panel of subject matter experts (SMEs). This SQA SME panel will consist of Federal employee representatives from Headquarters and Field Elements that have expertise in safety analysis, safety design, I&C, software development, and SQA. Persons who are not Federal employees will provide information and advice on an individual basis. The panel will assist the Department, and in particular, the EH "Office of Quality Assurance," in the specific areas of concern highlighted in Recommendation 2002-1. The panel will be tasked by EH to provide the following:

- Assistance, as requested, to support management's efforts in accomplishing this Implementation Plan;
- Programmatic input to EH regarding the development and implementation of an effective safety software quality assurance program;
- Expertise in safety analysis, design, and safety system software issues relating to safe design and operation of DOE nuclear facilities;
- A mechanism to identify and address major software issues that have crosscutting impact across the DOE complex;
- A forum for sharing ideas and proven processes or programs to both DOE and contractor management.

To facilitate continuous improvement in SQA and technology, the Department will identify a method of clearly communicating lessons learned, new technology, and innovative techniques that are related to safety software and SQA. This communication will be to both Federal and contractor personnel involved with safety software, and may utilize existing systems within DOE or a separate website dedicated to safety software and SQA. The SQA SME panel will also assist with this effort.

The software industry, and software technology, continue to grow and evolve, and there is much the Department can learn. Agencies such as the National Aeronautics and Space Administration and the Department of Defense, organizations such as the Software Engineering Institute, and industry groups, such as the Nuclear Utility Software Management Group and the American Society of Mechanical Engineers Code Committee for Nuclear Quality Assurance, all have a related interest in software issues and possess knowledge and expertise that can potentially benefit the Department. The Department will identify and establish relationships with outside groups, organizations, companies, and agencies that have an interest in SQA that are similar to that being addressed by this IP. The Department will actively participate with these groups and use these relationships to assist with benchmarking and sharing lessons learned and new technologies.

Deliverables/Milestones

Commitment 4.4.1: Establish a corporate QA function within EH that is responsible and accountable for the identification and resolution of Departmental crosscutting QA issues, such as SQA.

Lead Responsibility:	Assistant Secretary for Environment, Safety and Health
Deliverable:	DOE O 414.1A, *Quality Assurance*, revised to incorporate EH's roles and responsibilities
Due Date:	In accordance with schedule established in 4.3.2.1

Commitment 4.4.2: Identify methods for capturing and clearly communicating SQA lessons learned, new technology, innovative techniques, and areas in software development in which research and development is needed to ensure software quality.

Lead Responsibility:	Assistant Secretary for Environment, Safety and Health
Deliverable:	"Information sharing" mechanism functioning for SQA
Due Date:	October 2003

Commitment 4.4.3: Establish relationships and actively participate with outside groups, organizations, companies, and agencies that have an interest in SQA that is similar to that being addressed by this IP. This participation will assist the Department in benchmarking, research and development, and sharing of lessons learned and new technologies

Lead Responsibility:	Assistant Secretary for Environment, Safety and Health

Deliverable: Report describing relationships with outside groups, including points of contact

Due Date: December 2003

5.0 Organization and Management

Overall execution of this IP is the responsibility of the Assistant Secretary for Environment, Safety and Health. A Responsible Manager will be assigned to ensure individuals responsible for deliverables and commitments identified within this IP complete their actions. However, responsibility for implementing SQA rests with the line manager and they are responsible for many of the deliverables associated with commitments made within this IP. This includes ensuring that the necessary resources are provided. The various lead responsible organizations identified within the IP are accountable to the Assistant Secretary for Environment, Safety and Health with regard to the completion of deliverables.

5.1 Change Control

Complex, long-range plans require sufficient flexibility to accommodate changes in commitments, actions, or completion dates that may be necessary due to additional information, improvements, or changes in baseline assumptions. The Department's policy is to (1) provide prior written notification to the Board on the status of any IP commitment that will not be completed by the planned milestone date, (2) have the Secretary approve all revisions to the scope and schedule of IP commitments, and (3) clearly identify and describe the revisions and bases for the revisions. Fundamental changes to the IP's strategy, scope, or schedule will be provided to the Board through formal revision and reissuance of the IP. Other changes to the scope or schedule of planned commitments will be formally submitted in appropriate correspondence approved by the Secretary, along with the basis for the changes and appropriate corrective actions.

5.2 Reporting

To ensure the various Department implementing elements and the Board remain informed of the status of plan implementation, the Department's policy is to provide progress reports to the Board and/or Board staff. The Department will provide briefings to the Board and/or Board staff approximately every 4 months.

Commitment 5.2.1: The Department will provide briefings to the Board and Board Staff. These briefings will include updates on the status of completing actions identified in the various reviews and assessments indicated in this IP.

Lead Responsibility: Assistant Secretary for Environment, Safety and Health

Deliverable: Briefings

Due Date: June 2003, and approximately every four months thereafter

Table 1: Summary of Implementation Plan Commitments and Deliverables/Milestones

Number	Commitment	Deliverable	Due Date	Responsibility
1	Commitment 4.1.1: Issue a DOE Notice that identifies, documents, and communicates roles, responsibilities, and authorities for SQA by organizational element.	DOE Notice	July 2003	Assistant Secretary for Environment, Safety and Health
2	Commitment 4.1.2: Establish technical qualification requirements for Federal personnel whose duties and responsibilities require them to provide assistance, guidance, direction, oversight, or evaluation of safety software QA activities.	Software Engineer Technical Qualification Standard (or revision of an existing Qualification Standard)	November 2003	Chair, Federal Technical Capability Panel (FTCP)
3	Commitment 4.1.3: Identify the Federal positions whose duties and responsibilities require them to provide assistance, guidance, direction, oversight, or evaluation of safety software QA activities.	Technical Qualification Program (TQP) position list updated to include SQA positions	October 2003	Program Secretarial Officers (PSOs) and Field Element Managers
4	Commitment 4.1.4: Personnel assigned to SQA positions achieve qualification per the requirements of the Technical Qualification Program.	FTCP TQP Status Report that includes the identification of at least one qualified SQA position for each organization that requires qualified personnel.	September 2004	PSOs and Field Element Managers

Number	Commitment	Deliverable	Due Date	Responsibility
5	Commitment 4.1.5: Revise the FRAM to incorporate Federal responsibilities and authorities for SQA.	Approved FRAM Revision	December 2003	Assistant Secretary for Environment, Safety and Health
6	Commitment 4.1.6: Revise the Headquarters and Field Element FRA documents to incorporate Federal responsibilities and authorities for SQA.	Approved FRA Revisions	April 2004	PSOs and Field Element Managers
7	Commitment 4.2.1.1: Identify the codes used for safety analysis to be part of the Safety Analysis Code Toolbox.	List identifying the toolbox codes	Complete	Assistant Secretary for Environment, Safety and Health
8	Commitment 4.2.1.2: Establish SQA criteria for the safety analysis "toolbox" codes.	SQA plan (including criteria) for toolbox codes	July 2003	Assistant Secretary for Environment, Safety and Health
9	Commitment 4.2.1.3: Perform a gap analysis on the toolbox codes to determine the actions needed to bring the code into compliance with SQA qualification criteria and develop a schedule with milestones to upgrade each code based on the gap analysis results.	Schedule with milestones to upgrade each code based on the gap analysis results	November 2003	Assistant Secretary for Environment, Safety and Health
10	Commitment 4.2.1.4: Issue code-specific guidance reports on use of the "toolbox" codes identifying applicable regimes in accident analysis, default inputs, and special conditions for use.	Code-specific guidance reports provided to the Central Registry	September 2003	Assistant Secretary for Environment, Safety and Health

Number	Commitment	Deliverable	Due Date	Responsibility
11	Commitment 4.2.1.5: Conduct a survey of design codes currently in use to determine if any should be included as part of the toolbox codes.	Report on results of design code review	December 2003	Assistant Secretary for Environment, Safety and Health
12	Commitment 4.2.2: Establish and implement a Central Registry for the long-term maintenance and control of the safety analysis "toolbox" codes.	Memorandum from Deputy Secretary of Energy designating central registry	August 2003	Assistant Secretary for Environment, Safety and Health
13	Commitment 4.2.3.1: Develop criteria and guidance for the identification, selection and assessment of safety system software and firmware at defense nuclear facilities.	Criteria review and approach document (CRAD)	August 2003	Assistant Secretary for Environment, Safety and Health
14	Commitment 4.2.3.2: Establish a schedule to complete the identification, selection, and assessment of safety system software and firmware at defense nuclear facilities.	Schedule of assessments	October 2003	PSOs and Field Element Managers
15	Commitment 4.2.3.3: Complete the identification, selection, and assessments of safety system software and firmware at defense nuclear facilities.	Reports to the PSO indicating the results of the assessments, any concerns with the quality of existing I&C software, and the actions necessary to address the concerns.	In accordance with schedules established in 4.2.3.2	Field Element Managers

Number	Commitment	Deliverable	Due Date	Responsibility
16	Commitment 4.2.4.1: Develop criteria and guidance to assess the processes that are in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.	Criteria Review and Approach Document (CRAD)	August 2003	Assistant Secretary for Environment, Safety and Health
17	Commitment 4.2.4.2: Establish a schedule to complete the assessment of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.	Schedule of assessments	October 2003	PSOs and Field Element Managers
18	Commitment 4.2.4.3: Complete the assessments of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.	Reports to the PSO indicating the results of the assessments, any concerns with the quality of existing codes and the actions necessary to address the concerns.	In accordance with schedules established in 4.2.4.2	Field Element Managers
19	Commitment 4.3.1: Conduct a review to identify the industry or Federal agency standards that are appropriate for DOE safety software.	Report identifying appropriate industry or Federal agency standards.	September 2003	Assistant Secretary for Environment, Safety and Health
20	Commitment 4.3.2.1: Establish a schedule to develop, revise, approve, and issue required SQA directives.	Schedule to develop, revise, approve, and issue required SQA directives.	October 2003	Assistant Secretary for Environment, Safety and Health

Number	Commitment	Deliverable	Due Date	Responsibility
21	Commitment 4.3.2.2: Issue required SQA directives.	Approved directives in accordance with the schedule issued in 4.3.2.1	In accordance with schedules established in 4.3.2.1	Assistant Secretary for Environment, Safety and Health
22	Commitment 4.3.3: Headquarters and Field Elements review the approved SQA directives and determine the actions necessary to implement the requirements.	SQA directive Implementation Plan and schedule	Three months following issuance of SQA directives	PSOs and Field Element Managers
23	Commitment 4.4.1: Establish a corporate QA function within EH that is responsible and accountable for the identification and resolution of Departmental crosscutting QA issues, such as SQA.	DOE O 414.1A, *Quality Assurance*, revised to incorporate EH's roles and responsibilities	In accordance with schedule established in 4.3.2.1	Assistant Secretary for Environment, Safety and Health
24	Commitment 4.4.2: Identify methods for capturing and clearly communicating SQA lessons learned, new technology, innovative techniques, and areas in software development in which research and development is needed to ensure software quality.	"Information sharing " mechanism functioning for SQA	October 2003	Assistant Secretary for Environment, Safety and Health

Number	Commitment	Deliverable	Due Date	Responsibility
25	Commitment 4.4.3: Establish relationships and actively participate with outside groups, organizations, companies, and agencies that have an interest in SQA that is similar to that being addressed by this IP. This participation will assist the Department in benchmarking, research and development, and sharing of lessons learned and new technologies.	Report describing relationships with outside groups including points of- contact	December 2003	Assistant Secretary for Environment, Safety and Health
26	Commitment 5.2.1: The Department will provide briefings to the Board and Board Staff. These briefings will include updates on the status of completing actions identified in the various reviews and assessments indicated in this IP.	Briefings	June 2003 and approximately every 4 months after	Assistant Secretary for Environment, Safety and Health

Appendix A: List of Acronyms

CIO – Chief Information Officer

CRAD – Criteria Review and Approach Document

DOE – Department of Energy

EM – Environmental Management

EH – Environment, Safety and Health

FRA – Functions, Responsibilities and Authorities

FRAM – Functions, Responsibilities and Authorities Manual

FTCP – Federal Technical Capability Panel

NRC – Nuclear Regulatory Commission

PLC – Programmable Logic Controller

PSO – Program Secretarial Officer

QA – Quality Assurance

SCADA – Supervisory Control and Data Acquisition

SSC – Structures, Systems, and Components

SQA – Software Quality Assurance

TQP – Technical Qualification Program

USQ – Unreviewed Safety Question

USQD – Unreviewed Safety Question Determination

Appendix B: Glossary of Terms

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.

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

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]

Safety Analysis & Design Software – Computer software that is not part of an SSC, but is used in the safety classification, design, and analysis of nuclear facilities to:

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

Safety-class structures, systems, and components (SC SSCs) - Structures, systems, or components, 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]

Safety-significant structures, systems, and components (SS SSCs). Structures, systems, and components 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, safety-significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in a prompt worker fatality or 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 safety-significant SSC designation may be warranted. Estimates of worker consequences for the purpose of safety-significant 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 safety-significant SSC designation. [DOE G 420.1-1]

Safety Software – as referenced and defined in this Implementation Plan, includes both safety system software and safety analysis and design software.

Safety SSCs – The set of safety-class structures, systems, and components, and safety-significant structures, systems and components for a given facility. [10 CFR 830]

Safety System Software – Computer software and firmware that performs a safety system function as part of a 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, 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 function.

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

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.

Appendix C

Defense Nuclear Facilities Safety Board Recommendation 2002-1

[DNFSB LETTERHEAD]

September 23, 2002

The Honorable Spencer Abraham
Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Abraham:

The Defense Nuclear Facilities Safety Board (Board) has been following closely the Department of Energy's (DOE) response to a reporting requirement dated January 20, 2000, which requested a corrective action plan to address deficiencies documented in the Board's technical report DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities.* Although more than two years have since elapsed, DOE has been unable to develop and execute an acceptable plan to resolve these issues, some of which were identified as early as 1989. Since the Board's August 15, 2001, public meeting on quality assurance, DOE has been developing an overall Quality Assurance Improvement Plan that includes software quality assurance as a key element, but this effort has not yet produced any substantial results.

As a result, the Board on September 23, 2002, unanimously approved Recommendation 2002-1, *Quality Assurance for Safety-Related Software*, which is enclosed for your consideration. After your receipt of this recommendation and as required by 42 U.S.C. § 2286d(a), the Board will promptly make it available for access by the public in DOE's regional public reading rooms. The Board believes that the recommendation contains no information that is classified or otherwise restricted. To the extent this recommendation does not include information restricted by DOE under the Atomic Energy Act of 1954, 42 U.S.C. §§ 2161-68, as amended, please see that it is promptly placed on file in your regional public reading rooms. The Board will also publish this recommendation in the Federal Register.

Sincerely,

John T. Conway
Chairman

c: Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD
RECOMMENDATION 2002-l TO THE SECRETARY OF ENERGY
Pursuant to 42 U.S.C. § 2286a(a)(5)
Atomic Energy Act of 1954, As Amended

September 23, 2002

Background. Two core Integrated Safety Management (ISM) functions evolving from the Department of Energy's (DOE) implementation of Defense Nuclear Facilities Safety Board (Board) Recommendation 95-2, *Safety Management* are: (1) analyzing hazards; and (2) identifying and implementing controls to prevent and/or mitigate potential accidents. DOE relies heavily on computer software to analyze hazards, and design and operate controls that prevent or mitigate potential accidents.

DOE and its contractors use many codes to evaluate the consequences of potential accidents. Safety controls and their functional classifications are often based on these evaluations. Functional classifications establish the level of rigor to which controls are designed, procured, maintained, and inspected. The robustness and reliability of many structures, systems, and components (SSCs) throughout DOE's defense nuclear complex depend on the quality of the software used to analyze and to guide these decisions, the quality of the software used to design or develop controls, and proficiency in use of the software. In addition, software that performs safety-related functions in distributed control systems, supervisory control and data acquisition systems (SCADA), and programmable logic controllers (PLC) requires the same high quality needed to provide adequate protection for the public, the workers, and the environment. Other types of software, such as databases used in safety management activities, can also serve important safety functions and deserve a degree of quality assurance commensurate with their safety significance.

In some areas where there is at present no substantial activity in development of new software for safety applications, new calculations are usually based on existing codes, with data inputs and some logic chains often modified to fit the problems of the moment. It is therefore necessary to ensure that software so modified is not placed in general use in competition with generally validated and more widely useable software.

Software quality assurance (SQA) provides measures designed to ensure that computer software will perform its intended functions. Such measures must be applied during the design, testing, documentation, and subsequent use of the software, and must be maintained throughout the software life cycle. It is generally accepted that an effective SQA program ensures that:

- All requirements, including the safety requirements, are properly specified.
- Models are a valid representation of the physical phenomena of interest, and digital control functions are properly executed.
- Input and embedded data are accurate.

- Software undergoes an appropriate verification and validation process.
- Results are in reasonable agreement with available benchmark data.
- All internal logic states of PLCs and SCADA are understood, so that no sequence of inputs, even those due to component failure, can leave the controlled system in an unexpected or unanalyzed state.
- Computer codes are properly and consistently executed by analysts.
- Code modifications and improvements are controlled, subjected to regression and re-acceptance testing, and documented.

DOE identified inadequate SQA as a problem as early as December 1989, when its Office of Environment, Safety and Health (DOE-EH) issued ENVIRONMENT, SAFETY & HEALTH BULLETIN EH-89-9, *Technical Software Quality Assurance Issues*. This bulletin states, "Inadequate SQA for scientific and technical codes at any phase in their 'life cycle' may not only result in lost time and/or excessive project costs, but may also endanger equipment and public or occupational sectors." The bulletin cites problems with all three types of software noted above (analysis, design, and operation). Likewise, a 1997 assessment performed by DOE's Accident Phenomenology and Consequence Assessment Methodology Evaluation Program determined that only a small fraction of accident analysis computer codes meet current industry SQA standards. SQA problems continue to persist, as documented in the Board's technical report DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*, issued in January 2000.

An integrated and effective SQA infrastructure still does not exist within DOE. This situation can lead to both errors in technical output from software used in safety analyses and incorrect performance of instrumentation and controls for safety-related systems. In a letter to DOE dated January 20, 2000, the Board identified these deficiencies and requested that DOE provide a corrective action plan within 60 days. On October 3, 2000, the Board received DOE's corrective action plan, but found that it did not sufficiently respond to the Board's concerns. On October 23, 2000, the Board asked for a new plan of action; DOE has never submitted a revised plan, although several deliverables under the original plan have been received.

During the Board's August 15, 2001, public meeting on quality assurance, DOE proposed a revised set of actions to improve SQA processes and practices. Since then, DOE has attempted to develop a Quality Assurance Improvement Plan that includes SQA as a key goal. This action now appears stalled as a result of internal differences over objectives and funding. Thus, despite well over two years of effort, DOE has failed to develop and implement effective corrective actions in response to the Board's reporting requirement.

This situation is not acceptable. To improve SQA in the DOE complex, the Board recommends prompt actions to achieve the following:

Responsibility and Authority

1. Define responsibility and authority for the following: developing SQA guidance, conducting oversight of the development and use of software important to safety, and directing research and development as noted below. Roles and responsibilities should address all software important to safety, including, at a minimum, design software, instrumentation and control software, software for analysis of consequences of potential accidents, and other types of software, such as databases used for safety management functions.

2. Assign those responsibilities and authorities to offices/individuals with the necessary technical expertise.

Recommended Computer Codes for Safety Analysis and Design

3. Identify software that would be recommended for use in performing design and analyses of SSCs important to safety, and for analysis of expected consequences of potential accidents.

4. Identify an organization responsible for management of each of these software tools, including SQA, technical support, configuration management, training, notification to users of problems and fixes, and other official stewardship functions.

Proposed Changes to the Directives System

5. Establish requirements and guidance in the DOE directives system for a rigorous SQA process, including specific guidance on the following: grading of requirements according to safety significance and complexity; performance of safety reviews, including failure analysis and fault tolerance; performance of verification and validation testing; and training to ensure proficiency of users.

Research and Development

6. Identify evolving areas in software development in which additional research and development is needed to ensure software quality.

Appendix D
Department's Recommendation 2002-1 Acceptance Letter

[SOE LETTERHEAD]

November 21, 2002

The Honorable John T. Conway
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, D.C. 20004

Dear Mr. Chairman:

The Department acknowledges receipt of the Defense Nuclear Facilities Safety Board's (Board) recommendation 2002-1, *Quality Assurance for Safety-Related Software*, issued on September 23, 2002, and published in the *Federal Register* on October 9, 2002. The Department accepts recommendation 2002-l and will develop an Implementation Plan that results in the following:

- Clear assignment of organizational roles, responsibility, and authority for safety-related software.

- Creation of infrastructure necessary to ensure an effective software quality assurance program, including personnel with the appropriate skill and expertise.

- Implementation of processes to identify safety analyses and design codes and ensure that they are subject to verification and validation appropriate for the application.

- Establishment of requirements and guidance for a rigorous software quality assurance process, which will include the use of industry standards where practicable.

- Creation of a process that will track continuous improvements and initiatives in software technology. This information will be used as a basis for maintaining safety-related software and will be shared across the complex.

The Department has initiated activities to improve the implementation of quality management systems at its defense nuclear facilities. Many of these activities resulted from the deficiencies documented in the Board's Technical Report DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*, and discussed at several of your public meetings on quality assurance. The Department considers its efforts to improve software quality assurance as a key element in the overall improvement of our quality management system, and the Implementation Plan will include and build on the actions that were previously undertaken as part of this initiative.

Ms. Beverly Cook, Assistant Secretary for Environment, Safety and Health, is the Department of Energy official responsible for safety-related quality assurance and for ensuring the successful completion of the Implementation Plan we will develop in response to your recommendation.

Mr. Ray Hardwick, Office of Environment, Safety and Health, (301) 903-4244, is the responsible manager for the preparation of the Department's Implementation Plan.

Please feel free to contact either of them with any questions you may have as the Department moves forward with development of the Implementation Plan.

Sincerely,

Spencer Abraham